Managing Multiple Filings with Privacy Protection Authorities in Europe

Wim Nauwelaerts

Wim Nauwelaerts

When it comes to protecting individuals' personal data, the European Union imposes legal requirements and restrictions among the most stringent in the world. Specific legislation governing the collection, use, processing or disclosure of personal data and its free movement in Europe was introduced 10 years ago through adoption of Directive 95/46/EC (Privacy Directive). In the meantime, the Privacy Directive has been transposed into the national laws of the 25 EU Member States as well as three EFTA-countries (i.e. Iceland, Liechtenstein and Norway), jointly referred to as the European Economic Area, or EEA.

Divergence of National Data Protection Rules

EU directives are generally only binding on the result to be achieved, to the extent that Member States are free to choose the form and methods of implementing a directive in their national laws. Therefore, although the Privacy Directive may have harmonized the level of personal data protection granted to individuals residing in the EEA, the applicable rules in the Member States individually are far from uniform. As a result, the regulatory conditions for processing personal data in one Member State may be more onerous compared to those in another country, yet both sets of rules are based on the Privacy Directive. In addition, monitoring the application of these rules is left in the hands of the individual Member States, who created specific data privacy authorities for that purpose. There is no real enforcement action at the level of the European Union or EEA, apart from some sporadic initiatives of the so-called 'Article 29 Working Party,' an independent advisory body to the European Commission

comprising representatives of the national data privacy authorities.

To File or Not to File — That's the Question

In the EEA, companies that process personal data must, in principle, notify the privacy authority of the Member State where the processing takes place. The idea behind this notification requirement is that national supervisory authorities should be able to assess whether a particular processing operation presents risks to the rights and freedoms of their citizens. The organization in charge of processing personal data will typically file an information sheet with the supervisory authority, specifying the purposes of the data processing, the identity of the recipients of the data, the security measures in place to safeguard the data and possible transfers of the data outside Europe. For specific categories of processing likely to pose substantial risks to an individual's privacy (i.e. health-related data), some domestic laws require a formal opinion, authorization or permit by the competent data protection authority before the data can be processed lawfully. Failure to comply with the obligation to notify or obtain prior authorization may lead to fines imposed by supervisory authorities as well as privacy lawsuits.

Exceptions to the Rule

As a deviation from the general rule that local data privacy authorities should be notified, the Privacy Directive set outs extensive exemptions, and the application of those exceptions is left to the Member States' discretion. The exemptions allow data privacy authorities to focus on problematic processing operations such as those that are likely to jeopardize individuals' fundamental rights and freedoms. Consequently, almost all Member States have exempted certain categories of processing operations from the notification obligation, such as the processing of personal data for the purposes of keeping and updating public registers. Other exemptions include processing of personal data for journalistic purposes or for meeting specific legal requirements (i.e. to comply with tax laws). In most cases, non-profit organizations (founda-

"Failure to comply with the obligation to notify or obtain prior authorization may lead to fines imposed by supervisory authorities as well as privacy lawsuits."

See EU page 12

EU

continued from page 11

tions, associations, etc.) also are exempt from filing with the local data privacy authority.

Dealing with Different Domestic Approaches

Regardless of the notification principles set out in the Privacy Directive, a recent study by the European Commission shows that Member States keep different views on what types of processing operations are likely to adversely affect individuals' privacy rights, which makes a supervisory authority review essential. These different approaches have resulted in a complex web of domestic filing systems throughout Europe. Where for the same data-processing operation prior approval may be required in one Member State, a simple notification may suffice in another. For companies doing business in the EEA, compliance with applicable domestic filing and/or authorization requirements are often costly and time-consuming.

For example, a company that wants to process health-related personal data in Belgium must notify the local Privacy Commission, but would usually be able to start processing the data a few days later. In Italy, the same company would have to obtain prior approval from the local data privacy authority, which could take up to 45 days. In addition, separate files would have to be prepared for each country, observing different requirements in terms of content and form.

The Appointment of Data Protection Officers as an Alternative to Filing

So far, only five EU countries (France, Germany, Luxemburg, the Netherlands and Sweden) have appointed a Data Protection Officer ('DPO") to cut down on the red tape. The DPO-system is optional in these countries, except for Germany, where every private organization with more than four persons engaged in automated data processing is required to appoint a DPO. According to the German supervisory authorities, the system is beneficial to all stakeholders, as DPOs are aware of their organization's issues and may be able to solve data privacy problems most effectively. In addition, if a conflict arises between the organization and its DPO regarding privacy issues, the DPO could ask for support from the competent data protection authority.

In Sweden, if the Swedish Inspection Board has been informed about the appointment of a DPO, the general notification duty does not apply. However, the DPO is obliged to keep a register of the organization's processing activities, which should have been filed in the absence of a DPO. Under the Dutch system, each DPO is appointed a 'dedicated' contact person within the local supervisory authority, from whom the DPO could receive practical guidance on particular privacy questions or issues.

The DPO-system in Luxemburg is unique in that the DPO cannot be an employee of the organization — only third par-

ties, such as attorneys and IT consultants, are authorized to serve as DPOs.

Toward a One-Stop-Shop for Filing Purposes?

Experience shows that where the DPO system is in use, the level of data protection within the entities improves, while administrative burdens are kept to a minimum. However, at this moment the DPO system is available only in a handful of Member States. Meanwhile, in the other EEA countries, multinational companies still may have to submit individual files in each country where they process personal data. If prior authorization is required in several countries, the fact that the supervisory authority in one Member State grants approval does not guarantee that approval will be obtained elsewhere.

The European Commission's Article 29 Working Party has therefore suggested a simplified notification system, whereby an organization with cross-border processing operations would submit an extensive notification/file for review in one Member State. Provided the processing operation would receive the green light in that Member State, the supervisory authorities in the other relevant countries where similar processing operations take place would settle for a simplified notification. As a result, all stakeholders' interests would be served, while saving time. Although the proposal to introduce a 'one-stop-shop' filing system deserves praise, implementing it would likely require the Members States to amend their data protection- and privacy-laws. However, considering that it took some Member States more than eight years to transpose the Privacy Directive into their domestic laws, it is unlikely that any new major legislative initiatives would emerge in the near future.

Wim Nauwelaerts is a lawyer in the Brussels' office of Hogan & Hartson L.L.P., specializing in EU privacy and data protection law. He can be reached by email at wnauwelaerts@hhlaw.com or by telephone at +32 2 505 09 11.