Data protection developments in Central and Eastern Europe

On May 1 2004, ten countries joined the European Union as new Member States. While the media focused mostly on the radical transformation of the EU's geographical boundaries, the impact on the EU's data protection regime was no less significant.

Accession: a work in progress

The lengthy bilateral negotiations between the EU and each of the candidate countries were meant to ensure that on 1 May 2004 each candidate had aligned its laws with the EU's *acquis communautaire*, including its rules relating to data protection. In the eleventh-hour negotiations preceding May 1, none of the candidates requested a transition period to implement the EU's directives regulating the processing of personal data and therefore, in theory at least, the data protection laws of each were meant to be consistent with the EU's on that date.

In reality, many candidates fell short of full alignment. This is perhaps unsurprising. By the time the European Commission released its final Accession Reports for each candidate in October 2003, it recognized two types of candidate: those whose data protection laws, while "largely aligned" with the EU's, needed further refinement, such as Hungary, the Czech Republic, and Poland, and those whose laws needed more extensive revision.

Also in its Reports, the Commission felt compelled to bring a second, more fundamental issue to the attention of certain candidates: structural reform. The Commission was concerned that some national privacy regulators lacked adequate resources, and more importantly, real independence from other government institutions to have freedom to act in a manner comparable to privacy regulators in the EU. Although most candidate countries did satisfy the Commission in this regard before release of the final October 2003 Accession Reports, the Commission found that some, such as Estonia and Latvia, still had further to go.

What was the position on May 1? Despite expending a great deal of effort, many of the Commission's concerns remained unaddressed when the candidate countries became new Member States. Some countries, such as Poland and Hungary, did manage to enact legislation responsive to the Commission's concerns, whereas others, like the Czech Republic, Slovakia, and Slovenia, had prepared, but not yet passed, draft legislation. Other candidates, meanwhile, were further behind in their reform efforts. In the coming months, the Commission will assess the performance of each new Member State, and, undoubtedly, engage in further consultations in a number of cases. For those new Member States that prove recalcitrant, Commission-initiated infringement proceedings remain a distinct possibility in the future.

Issues in compliance

Today, organisations doing business in the new Member States will need to tread cautiously, and should not assume that a particular country has fully or even accurately transposed the EU's data protection regime. Even where national data protection laws have been successfully aligned, differences in the application and interpretation of those laws undoubtedly will emerge.

In fact, national variations on key data protection issues already are apparent. Some of the more notable include:

- Security: some new Member States have crafted detailed local security rules governing the manner by which personal information may be processed, whereas others apply a broader standard;
- Data transfers: some new Member States require that organisations seek prior approval before transferring personal information from the jurisdiction to destinations outside the EU, although others do not;
- Compliance officers: some, but not all, of the new Member States require or recommend that organisations appoint independent data protection officers;
- Consent: the new Member States appear to be adopting different approaches and attitudes on the issue of data subject consent and how organisations can procure valid consents; and
- Sanctions: the penalties potentially applicable for breaching local data privacy laws differ widely among the new Member States, as do the enforcement powers of privacy regulators. Whereas some regulators can impose significant administrative fines, others cannot and must refer serious cases to other enforcement bodies.

Benefits of accession

For organisations doing business in the enlarged EU, transfers of personal data to and from the new Member States should be considerably easier in future. This includes transfers of personal information between organisations acting as two independent controllers, as well as transfers from a data controller to its data processor.

Organisations prior to accession typically would have entered into a data processing agreement robust enough to satisfy Article 17(3) of Directive 95/46/EC (requiring controller-processor agreements), as well as Article 25 (requiring

adequate protection for transfers to third countries), with their processors in the new Member States. These contracts tend to be quite onerous, as evidenced by the EU Commission's own standard contractual clauses. Because Article 25 no longer applies in these circumstances, organisations can use a less burdensome agreement that simply satisfies Article 17.

Relatedly, accession should facilitate data flows *to* organisations located in the new Member States - whether affiliates, subsidiaries or business partners - functioning as independent data controllers. In the past, it would have been necessary for organisations in the EU either to deploy a robust data transfer contract, obtain the consent of the data subject, or find some other method for complying with the Article 25 transfer restriction, making such transfers troublesome in practice. Often, organisations found it easier to simply embargo data flows to affiliates and subsidiaries located in the new Member States. Since May 1, the transfer of personal information can take place without having to rely on a contract, consent or some other device.

Accession should also make it easier to transfer data *from* the new Member States. Prior to accession, some countries, notably Hungary, had cross-border transfer rules more restrictive than the EU's. Those obstacles have now been removed. Nevertheless, organisations may find themselves confronted with some challenging issues as they abandon their former transfer mechanisms.

Emerging enforcement trends

Organisations meanwhile should take heed as the enforcement of national data protection laws continues apace in each of the new Member States. National privacy regulators, spurred by a regular flow of complaints and greater public awareness, are showing themselves increasingly active in enforcing their local data protection rules. Interestingly, a high proportion of their enforcement targets have been public bodies and government agencies, and regulators are showing themselves to be particularly strident government watchdogs.

Today, organisations doing business in the new Member States will need to tread cautiously, and should not assume that a particular country has fully or even accurately transposed the EU's data protection regime

Poland's Inspectorate General is a good example of how active regulators can be, having in 2003 performed over 180 inspections of organisations suspected of breaching Poland's data protection statute. The Czech Office of Personal Data Protection, which conducted over 60 inspections in each of the past two years, appears slightly more representative. A high percentage of reported cases involve fairly fundamental breaches of the law - failures to file notifications, excessive processing of personal information, undisclosed processing, and inadequate security - suggesting that local organisations either may be struggling to comply or do not yet regard enforcement to be a real risk.

Sanctions and penalties for non-compliance, on the other hand, largely have been modest to date, and self-correction, warnings, and the discontinuation of unlawful processing activities are popular remedies. Monetary sanctions - at least significant ones - remain scarce, even in jurisdictions like the Czech Republic, where regulators can impose administrative fines directly on organisations that breach the law. The filing of civil complaints remains uncommon, but that may soon change as individuals increasingly become aware of their rights and more confident in pursuing legal claims.

Further, certain industry sectors and activities are attracting greater regulatory attention than others. As previously noted, privacy regulators, especially in Hungary and the Czech Republic, have not shied away from regulating other government bodies at the local and national level. This includes police and law enforcement bodies, health authorities, social security and benefits agencies, political parties, and other agencies handling large volumes of personal information. In the private sector, on the other hand, familiar subjects of regulatory scrutiny include banks and financial institutions, insurance providers, healthcare providers, telecommunications providers, and direct marketers. Organisations that routinely handle large volumes of personal information should regard themselves particularly at risk.

Conclusion

Accession has brought its fair share of challenges to organisations doing business in the new Member States. What should organisations expect now that the dust has settled? First, a number of the new Member States will enact new laws, and modify old ones, to complete the process of alignment. It is too early to tell whether the European Commission will intervene, but it may. Second, even where satisfactory national privacy laws are already in place, national regulators, prosecutors and judges will need to work their way through all of the interpretive questions that these laws will raise. Third, just as the experience with the EU's Directive 95/46/EC in the pre-accession EU has shown, legislative alignment - when it does take place - will not prevent national variations from emerging in the new Member States and complicating life for those seeking to comply.

Dan Cooper Senior Associate
Covington & Burling
dcooper@cov.com