EU enlargement extends data protection controls

Ten new countries from Central and Eastern Europe have joined the European Union, signalling major changes to the region's data protection landscape.

On May 1st, the European Union stretched out its borders, extending its reach into Central and Eastern Europe through the accession of ten new member states (see box, right).

One of the pre-accession conditions for entry into the EU was for candidate countries to align their domestic legislation with European law. All new member states were therefore required to bring in legislation that reflected requirements set out in the EU's 1995 Data Protection Directive.

The subsequent developments leading up to the May 1st accession date have resulted in significant legislative changes that will have a major impact on multinationals' compliance obligations. Many global companies have a presence in at least one of the ten accession countries, and the region has also become an attractive outsourcing location for western businesses. According to AT Kearney's *2004 Offshore Location Attractiveness Index*, Poland and Hungary fall within the top 11 outsourcing destinations, while the Czech Republic is ranked fourth, behind Malaysia, China and India.

Pre-accession status

While significant changes were needed to bring the candidate countries up to EU standards, according to Dan Cooper, lawyer at Covington & Burling, data protection regulation was certainly not a new concept to the region. Speaking at Privacy Laws & Business' Annual International conference in July, he explained that "a lot of these countries already had very mature data protection regimes before they even thought about entering the EU."

Poland's data protection law, for example, dates back to 1997, while Hungary's 1992 was given 'adequacy' status by the European Commission in 2000.

However, Cooper explained that although there were some strong data protection regimes in place, other candidate countries fell short of the directive. Even in those countries with strong data protection laws, there were legislative changes needed to ensure they were properly aligned with the EU directive.

> As well as a failure to fully implement the directive, there are a number of signficant variations between local laws.

Structural reforms were also required to ensure that data protection legislation was interpreted and enforced effectively. Some national data protection authorities, for example, did not have sufficient budgets or independence from their governments.

To address these problems, the European Commission established a number of tools to help the alignment process. These included support from the Commission's Technical Assistance and Information Exchange (TAIEX) unit, as well as funding from the Phare programme. The Phare programme set up a twinning process, which paired data protection authorities from existing EU member states with regulatory authorities in the candidate countries. The idea was to share experiences of interpreting and enforcing European data protection law.

Other alignment measures for the accession countries included observer status on the EU's Article 29 Working Party (a policy group representing European data protection authorities), as well as involvement with the OECD's data protection advisory committee.

Data protection authorities

Cyprus
Commissioner for Personal Data Protection
Contact: www.dataprotection.gov.cy

Czech Republic
The Office for Personal Data Protection
www.uoou.cz

Estonia
Estonian Data Protection Inspectorate
Contact: urmas.kukk@dp.gov.ee

Hungary
Data Protection Commissioner of Hungary
Contact: http://abiweb.obh.hu/abi/

Latvia
State Data Inspection
Contact: www.dvi.gov.lv

Lithuania
State Data Protection
Contact: www.ada.lt

Malta
Office of the Commissioner for Data Protection
Contact: www.dataprotection.gov.mt

Poland
The Bureau of the Inspector General for the Protection of Personal Data
Contact: www.giodo.gov.pl

Slovakia
Office for Personal Data Protection
Contact: www.dataprotection.gov.sk

Slovenia
Deputy Ombudsman
Contact: jernej.rovsek@varuh-rs.si

Post-accession status

So now that the ten countries have joined the EU, what is the status of data protection regulation in Central and Eastern Europe? Cooper explained that while there had been "excellent work done" by some accession states to meet the May 1st deadline, there is currently still a "patchwork of implementation" across the region. As well as a failure to fully implement the directive, there are a number of significant variations between local laws.

Take for example, the directive's requirement for organisations to notify or register their data processing activities with national data protection authorities. The original 15 EU member states failed to reach a consensus on this issue, and it is a problem that has been repeated in the accession countries. "The notification requirements in all these countries differ," said Cooper. "I've not seen a standard form that's been applied throughout the region."

> "The notification requirements in all these countries differ. I've not seen a standard form that's been applied throughout the region."
>
> **- Dan Cooper, Covington & Burling**

There are also discrepancies over data transfers, for example. While some data protection authorities require prior approval for data transfers outside the EU, others do not. In some accession countries, specific rules on data security have been created meaning that companies will be unable to rely solely on the more generic security requirements set out in the EU directive.

It is a similar situation with the implementation of the the EU's 2002 E-privacy Directive, which addresses issues such as unsolicited e-marketing and spyware technologies. While some of the accession countries have fully implemented the directive, others have only partially done so. Some have completely failed to implement it.

Cooper said that the gaps in implementation could cause problems when it comes to interpreting compliance with the law, especially considering that the courts have had little experience in dealing with data protection cases.

Commercial benefits

But, while there are still teething problems to be resolved, Cooper said that companies will derive some benefits from the accession process. The fact that their data protection laws have moved closer to the EU directive will be advantageous for companies trying to implement a pan-European or global privacy compliance strategy "At least on a superficial level, you can be relatively sure that as you go and do business in each of these new member states, the laws are roughly going to be harmonised with those you are used to dealing with in Europe."

Another key benefit, of course, is that now these countries are part of the European Union, businesses can bypass the rigid restrictions imposed on the export of data outside the EU. Cooper said previously, many organisations would simply choose to embargo the transfer of data to their Central and Eastern European operations. But with the restrictions lifted, these companies are now able to bring these units into their pan-European compliance regimes.

The accession process should also provide a boost to the outsourcing sector, removing the need for companies to rely on the strict provisions laid out in the European Commission's standard model contracts when passing data on to third party processors. For existing outsourcing relationships, Cooper said there "should be an opportunity to look at these contracts, revise them, and maybe negotiate a bit more flexibility with your outsourcing partners."

Enforcement trends

Cooper said that the data protection authorities in accession countries are becoming increasingly active, although the level of activity and sanctions available vary between countries. Hungary's data protection authority, for example, has only recently been empowered to carry out audits and inspections, while Poland is renowned for the number of inspections it carries out - in 2003 the Polish data protection authority conducted close to 200 inspections.

Non-compliant organisations could also find themselves faced with severe enforcement sanctions. "Slovakia and the Czech Republic do have serious financial penalties," said Cooper. The Czech Republic for example, can hand out fines of up to 10 million Czech crowns (around $400,000 or €320,000)

Cooper also highlighted the role of the media which is "bringing cases and complaints to the local regulators - much more than we are seeing in the West."

Fortunately, for the business community, data protection authorities have tended to focus more on public sector compliance, although Cooper said that commercial sectors such banking, insurance, and direct marketing have been the subject of investigations.

Future developments

While there is a high degree of variation between the accession countries' data protection laws and the EU directive, Cooper explained that the situation will improve. "We are going to see greater consistency in application as these laws get bedded down in their local regimes," he said.

How long this will take, and how patient the European Commission will be, is uncertain. "The interesting question," he said, "is whether the Commission will get involved to prod or compel some of those member states to do what they should have done before May 1st."

AUTHOR:

Alan Pedersen, Editor, *PL&B International*.

FURTHER INFORMATION:

European Commission's data protection website: http://europa.eu.int/comm/internal_market/privacy/index_en.htm

French data protection law, continued from p.3

The law has maintained the earlier system whereby the controller can implement data processing only after having received a receipt from the CNIL, which the CNIL is required to deliver promptly.

Although the law does not give a precise time limit to the CNIL, in order to meet company requirements, a prompt reply should be a matter of days. However, the CNIL is facing a large number of notifications and, whereas simplified notifications receive their receipts a few days after filing, ordinary notifications may have to wait between a few weeks and a few months, depending on the workload of the concerned CNIL department.

Prior authorisation

The new law has implemented a drastic change for the private sector in introducing an obligation to obtain the CNIL's authorisation for any processing operations that are likely to present risks to the rights and freedoms of individuals. For example:

- Automated or non-automated processing of sensitive data carried out in the public interest or when the data is intended to be promptly anonymised.

- Automated processing of genetic data, except if carried out by healthcare professionals or biologists and needed for preventive medicine, medical diagnosis, or provision of care and treatment.

- Automated or non-automated data processing of criminal offences and sanctions.

- Automated data processing which may exclude a person from the benefit of a right, a service or a contract, except as otherwise provided by law or regulation.

- Processing involving the national identification number, or a search of the national identity registry.

- Automated processing including assessment of people' social difficulties.

- Automated processing involving the interconnection of files which have different purposes; or

- Automated processing including biometric data necessary for ID controls.

The CNIL shall provide its reply within a two month-period which can be extended for a further two months by a grounded decision of its president. Unfortunately for diligent data controllers, if the CNIL has not issued an opinion within this timeframe, the request is deemed rejected.

This provision will, in particular, have an important impact on credit blacklists maintained by companies.

Rights and obligations

The law is very similar to the directive in most respects, although a few variations are worth describing.

Information requirements

The new law extends the scope of the notice to be provided to individuals, not only beyond the previous system, but much further than the directive's requirements. This will not provide much help to organisations which want to keep their data protection notices brief.

The data protection notice must include the identity of the controller - or its representative - and the data processing purposes, which are the two information categories required by the directive.

However, the controller must also include categories which, under the directive, would be provided only if required by the fair processing principle. These include whether data requested is mandatory or optional and the consequences of failure to provide it, and the data recipients or categories of data recipients (other than suppliers and people in charge of the data processing).

Additionally, individuals must be informed of their legal rights. That not only includes the right of access and rectification, but also the right of objection (on legitimate grounds or objection to solicitation) and the right to obtain information about automated decisions.

> Rather than referring to direct marketing, the new law uses the more general term of "solicitation".

Lastly, the notice must specify any data transfers outside of the European Community. Regrettably, this provision does not make any distinction between transfers to "adequate" and "non-adequate" countries, which may cast doubt in the mind of individuals as to the legality of the transfer. Data controllers will also, as a result of this provision, have to disclose data transfers even if they are made for adminstrative purposes under sufficient safeguards, such as contractual clauses concluded with outside service providers.

It should be noted that when questionnaires are used to collect data, only certain information categories have to be provided.

It is in the new data protection law (Article 32(2)) that the legislator has decided to implement the provisions of the EU Electronic Privacy & Communications Directive which apply to online technologies such as cookies and spyware. Other provisions of this directive, however, have been implemented under the law on confidence in the digital economy, adopted on June 21st 2004.

Access rights

Access rights have always been a pillar of French data protection law. In order to ensure that a controller does not destroy or hide personal data relating to an access request, individuals are given the opportunity to bring an emergency procedure

An important breakthrough which has been brought in by the law, acknowledges that protection for exported data can be provided, not only by contractual clauses, but also by internal company rules.

before the "juge des référés". On the other hand, to protect controllers from abusive requests, the legislator has given them the right to refuse requests which are obviously abusive, in particular by their volume or frequency. However controllers bear the burden of demonstrating the abuse in case of dispute.

Transborder data transfers

There was a real need to improve the 1978 law on this issue, as the CNIL's powers were very unclear. The new law prohibits data transfers to non-EEA countries which do not provide a "sufficient" level of protection. One may wonder about the legislator's choice of the term "sufficient" rather than the "adequate" terminology used in the directive, but hopefully it will not lead to differences in interpretation.

The exceptions to this prohibition mirror those of the directive, for example, individuals' consent, if the transfer is necessary for the performance of a contract between the controller and the individual, or for the exercise or defense of legal claims.

In any other circumstance, it is in the CNIL' sole authority to authorise a data transfer. To be authorised, the processing must ensure a sufficient level of protection.

An important breakthrough which has been brought in by the law, acknowledges that protection for exported data can be provided, not only by contractual clauses, but also by internal company rules. Had the law been adopted several years ago, at a time where the issue of binding corporate rules was not so current, this innovative provision would not have been enacted.

Enforcement

While the CNIL already had investigatory and control powers, it clearly lacked strong enforcement powers. Only in few instances did the CNIL bring cases to the attention of the public prosecutor and cases usually ended with very low fines in comparison with the maximum level set by the criminal code.

The new law gives the CNIL strong means to ensure compliance. The CNIL can still send warnings to controllers, and can also send a formal notice to stop unlawful processing to companies in breach of the law. If the alleged infringer is reluctant to comply, the CNIL can now issue sanctions (up to €150,000 and €300,000 in case of repetition within 5 years) and issue cease and desist orders or withdraw the authorisation it has granted.

The CNIL can now issue sanctions (up to €150,000 and €300,000 in case of repetition within 5 years) and issue cease and desist orders or withdraw the authorisation it has granted.

The CNIL cannot destroy unlawfully processed data, or the means for processing it. Because of the irrevocability of this type of action, such decisions are left to the judges. However, the CNIL can order the interruption of the processing or the blocking of some data elements for a maximum of three months in extreme cases, for example, if there is a violation of civil liberties, privacy and human rights.

Adverse publicity is also a powerful compliance tool. The CNIL may decide to make its warnings public. It may also order the publication of the sanctions it has ordered in newspapers and other media.

In order to ensure due process of rights, defendants will be able to present their arguments before the CNIL during the legal procedure.

The coming months will tell us if the CNIL, which was known for favouring dialogue with organisations, will change from a conciliatory approach to a more aggressive one.

The coming months will tell us if the CNIL, which was known for favouring dialogue with organisations, will change from a conciliatory approach to a more aggressive one.

Conclusion

The new French law is now in line with the directive. There are some slight differences in the wording adopted, the French Parliament preferring to use other adjectives than those of the directive or adopting a more simplified language. The future will tell us if they justify a difference in interpretation.

Controllers operating in French territory through an establishment of any type and controllers located outside of France but using data processing means on French territory (except for transit purposes) must comply with French law.

However, controllers who were lawfully operating automated data processing before the implementation of the law are given three years to bring themselves in line with the new provisions, and until October 24th 2007 for non-automated processing. However, the articles on objection rights, on transborder data flows and on the CNIL's investigatory and sanction powers are immediately applicable to existing data processing. Data processing that has already been notified does not require additional notification to the CNIL, unless changes made to the processing to ensure compliance, trigger changes to the features of the processing which was previously notified.

AUTHOR:

Pacale Gelly, Avocat à la Cour, specialising in data protection law

CONTACT:

pascalegelly@wanadoo.fr

FURTHER READING:

Details on the new law can be found on the CNIL's website: www.cnil.fr