Greece is the last EU member state to adopt a data law but first to implement the EU DP Directive

Hot on the heels of Mediterranean neighbours Italy, Greece adopted its own Data Protection Law on 10 April 1997, thus ensuring that all fifteen of the European Union's member states now have legislation on the statute books.

The law had been eagerly awaited ever since the Greek government took the unusual step, in August 1995, of ratifying Council of Europe Convention 108 without having legislation in place. However, this relaxed approach to its treaty obligations has allowed the Greek government the necessary time to draft a law intended to meet not only the requirements of the Convention but also those of the EU directive. Greece may be the last member state to adopt data protection legislation, but it has succeeded in implementing the directive some 18 months ahead of schedule, well ahead of all of its EU partners.

The legal clarity of a true 'framework' approach

Those who have a working knowledge of the EU directive will immediately see the similarities in the approach taken by the Greek legislator. The law does not follow exactly the same structure, (provisions on notification and third country transfers appearing earlier with sanctions and liabilities being grouped together at the end), but all of the main provisions of the directive are to be found. The overall 'framework' approach of the directive, establishing horizontal rules applicable irrespective of the economic sector or the form in which the data is held, is also faithfully respected, and is even taken a step further in the Greek law than was possible at Community level.

Directive's provisions apply to areas outside community law

Such a clear framework is the result of two bold choices taken by the legislator. First is the decision to apply the provisions of the directive not only to areas covered by Community law, but also to areas such as defence and police activities, which fall outside the scope of community powers, and therefore outside the scope of the directive itself. This is an important decision, and one which may have an influence on other governments, not least the new Labour administration in the UK, currently grappling with the same question. The directive, it should be remembered, does not affect Member States' approach to data protection in sectors falling outside community law. Governments, therefore, have a totally free hand in this area. However, traditionally the tendency across Europe has been for national laws to cover all sectors equally. In maintaining this tradition when implementing the directive, Greece has set a useful and very welcome precedent. To go down the alternative route, and set out separate provisions for sectors within Community law to those outside, would perhaps be popular with lawyers, but for everyone else (data subjects, data controllers, and supervisory authorities alike), it would clearly be a recipe for confusion.

Wider definition of manual data

The second decision relates to the law's provisions on manual data. Like the directive, the Greek law covers any processing of personal data carried out in whole or in part by automated means as well as the non-automated processing of personal data included, or to be included, in a filing system. What is interesting, however, is the definition of "filing system" included at article 2(e), according to which a filing system is simply a "group of data of a personal nature which constitute or may constitute the subject matter of processing." This is a much wider definition than that found in the directive, which talks of a structured set of personal data, easily accessible according to specific person-related criteria. It seems likely, therefore, that almost all manual data will fall within the Greek law.

The result of these two decisions is a comprehensive data protection framework, covering all personal data processing in all sectors (other than processing carried out for purely personal or household purposes), irrespective of whether that processing is automated or otherwise.

Geographical scope of the law - consistent with the Internal Market?

The basic rule on the geographic scope of the law follows the principle set out in the directive that national laws should apply to data controllers

established in the Member State in question. However, according to Article 3(3)(b), the Greek law will also apply whenever processing relates to persons established on Greek territory (Greek residents presumably), in which case the data controller must appoint a representative domiciled in Greece.

The striking aspect of this provision is that it will affect data controllers established in other EU Member States in the same way as those established in non-EU countries. Both will be subject to Greek law insofar as they process data about Greek residents. There may be doubts as to whether this complies with the directive's provisions on national applicable law and the principle of home country control favoured in Brussels as a means of ensuring that Member State laws do not overlap.

The Data Quality Principles: no 'compatibility' rule, but specific provisions on data matching

Article 4 contains the data quality principles found in Article 6 of the directive and Article 5 of Convention 108. The classic principles are present: data must be collected for specified, explicit and lawful purposes and subsequently processed fairly and lawfully; data must be adequate, relevant and not excessive; it must be accurate and up to date, and not kept for longer than necessary.

A notable omission (in the English translation at least) is the principle that further processing should be for purposes 'not incompatible' with the original purpose for which the data is collected. The absence of a rule dealing specifically with the key issue of secondary use is a little surprising. The French translation does, however include the term 'compatible', so this may simply be a language problem.

In any case, by way of compensation, the law includes an entire article on 'interconnection of files' to address the issue of data matching. Under this article, all proposed interconnections must be declared to the supervisory authority. Where the interconnection involves files including *sensitive data* or if a *uniform identity or code number* is to be used, then the supervisory authority must give permission in advance for the data matching to go ahead.

Consent of the data subject: the starting point for legitimate processing

Articles 5 and 7 of the law correspond quite closely to Articles 7 and 8 of the directive covering the grounds for processing data legitimately and the specific conditions for sensitive data.

In substance, Article 5 mirrors the directive in setting out six alternative grounds for processing. However in style it is different, placing great emphasis on the first of these grounds, consent. Consent is separated out into its own paragraph to emphasise its status as the basic requirement. Then a further paragraph includes the five other processing grounds (contract, legal obligation, vital interest of the data subject, public interest, balance of the controller's legitimate interest with that of the data subject) as possible 'exceptional' grounds when there is no consent.

Article 7 starts with a prohibition on the processing of sensitive data, and then includes consent (which must be written) as the first exemption from this rule. Further exceptions similar to those found in Article 8 of the directive follow. It is notable that only two "significant public interest" exemptions (permitted under Article 8(4) of the directive) are to be found. The first is for reasons of scientific research, providing anonymity is observed, and the second, and last, is for reasons of national security as well as for the purposes of criminal or correctional policy. A journalistic exemption in respect of sensitive data about public figures is also included.

The most radical provision in Article 7, however, concerns procedure rather than substance. It is the requirement for a permit from the supervisory authority before sensitive data can be processed. Such permits shall be granted for a limited period of time and may be subject to conditions. They shall be granted only after the controller and the processor have been summoned before the supervisory authority.

Rights of the data subject

In the area of individual rights the Greek law also has its own distinctive approach. The obligations on data controllers to provide *information when data is collected* are considered as data subject rights. Unlike the directive, however, no distinction is made between situations where data

is collected directly from the data subject and those where collection is made from a third party. As regards the content of the information to be given, the list is slightly longer than that set down explicitly in the directive, and additional information must be given if the data subject is asked for 'assistance' in the collection, as would be the case in an opinion survey, for example.

The right of access is dealt with more conventionally. Subject to a fee, to be decided by way of a regulation of the supervisory authority, the data subject has a right to:

- know whether he is the subject of data processing
- know the purposes of such processing and any categories of recipients of the data
- receive a copy of all the personal data and information as to the source of the data
- be told of the logic of the processing and
- of any changes to the processing that have taken place since information was last given to the data subject.

National security and the detection of crime are the only grounds for exemption here. No journalistic exemption is provided, a little surprisingly given the strong principle of confidentiality on the basis of which journalists protect their sources. The Greek authorities apparently considered the issue and took the view that the right of access was unlikely to infringe freedom of expression.

The right to have data rectified is grouped together in a separate article with *the right to object to processing,* a right which is of much broader application here than in Article 14 of the directive. There are additionally specific provisions guaranteeing *judicial protection for individuals subjected to automated individual decisions* based on personal profiles.

One significant omission with regard to the rights included in the directive is that there is no duty to inform third parties to whom inaccurate data had been previously disclosed of corrections to that data.

Transborder data flows - no provision for contractual solutions

For transfers of personal data to non-EU countries, the law, like the directive, requires there to be an adequate level of protection ensured by the destination country, subject to a limited series of exceptions. A permit from the supervisory authority is required, confirming adequacy of protection or that an exemption applies, before the data can be transferred.

No provision is made for contractual solutions in the absence of adequate protection. Of course, the directive does not require Member States to make such a provision (it is simply an option), but the absence of such a possibility will certainly raise eyebrows among those in the US-based business community who currently see contractual measures as the panacea to problems of privacy protection in international data flows.

Notification of Processing to the Supervisory Authority: A Universal Requirement

While the tendency in most countries with well-established data protection laws has been to seek to reduce dependency on formal registration or notification procedures, the Greek law shuns the possibility for exceptions and simplifications to such procedures offered by the directive, in favour of a system of universal notification. All data controllers must inform the supervisory authority in writing of their name, address, and a list of enumerated details regarding the processing in question. These details are included in a public register kept by the Data Protection Authority.

Remedies, Liabilities and Sanctions

The Greek law includes an impressive array of detailed provisions on sanctions, which may be administrative or criminal, as well as on civil liability for damage caused.

Criminal sanctions apply principally to failure to respect the need to register and receive permits from the supervisory authority, as well as to breaches of the rules on security and non-respect of the authority's decision regarding subject access. Where such offences are committed negligently, imprisonment is a possibility. The ability of an individual to obtain a judicial remedy for any breach of the law's substantive provisions does not appear clearly in the text, but can perhaps be implied by the provisions on sanctions and civil liability, when they are taken in the context of the general rules and principles of Greek penal and civil law.

The All-Powerful Supervisory Authority

No less than six articles (in a law which in total contains only 26) are dedicated to the establishment and operation of the Data Protection Authority. The Authority will comprise a chairman and six ordinary members, and will enjoy 'functional and personal independence.' It will be supported by a secretariat, the details of which will be decided by Presidential decree.

The first point to make about the Authority is that it has very significant powers. It can itself impose administrative sanctions, and in respect of criminal offences it can in certain circumstances proceed itself with the preliminary investigation. The Authority and certain of its employees have the status of 'special investigating officers' under the Greek code of penal procedure.

The second point to make is that the Data Protection Authority has a very extensive number of tasks. It must give recommendations and instructions to data controllers, assist in the preparation of codes of practice, indicate infringements of the law to the judicial authorites and impose administrative sanctions. It must additionally hear complaints and investigate them, issue regulations on the detailed application of the law, and compile an annual report for Parliament.

However, what is even more striking is the amount of direct supervisory work required of the Authority. No less than six registers must be maintained:

1. the basic register of processing operations (which will include *all* entities which process data)
2. the register of permits for holding sensitive data
3. the register of permits for interconnection of files
4. a register of persons who do not wish to receive mailings (a mailing preference list)
5. a register of permits for transfers of data outside the EU (a permit being required even where an exemption is claimed) and
6. a register of secret files held for defence and national security purposes.

By any measure this is a heavy burden of work likely to require large amounts of resources.

Conclusions

The Greek law will enter fully into force once the supervisory authority, to be appointed by Parliament on the basis of a proposal from the Minister of Justice, is in place.

The law is ambitious. Its scope goes beyond that of the directive, and its substantive provisions are wide-ranging yet relatively simple. Exemptions and caveats are few, allowing the law to be clear and easy to understand. For all of this, the Greek legislator is to be applauded.

But in terms of its procedural solutions, the law does look a little naïve. Universal registration, together with what is effectively a prior licensing system for the processing of sensitive data and for the export of data to third countries, may seem logical on paper, but in a world of modern telecommunications where even the smallest business uses a PC often connected to a global network, the practicality of such close supervision may be questionable. The worry is that the new supervisory authority will be so overwhelmed with notifications and requests for permits, which raise no real privacy concerns, that it will be unable to focus on the issues of major importance.

Such doubts should not detract from the Greek achievement in getting its data protection law on the statute book, and in doing so some 18 months before the deadline imposed by the EU directive. As the first national law that claims to implement the directive (the Italians still have a few modifications to make), the text is of more than passing interest to those working on their own national laws in the EU's other capital cities. Greece has seized the opportunity provided by the directive to create a bold new law, which should have a major impact on individuals and organisations throughout the Hellenic Republic. It remains to be seen if other Member States take an equally brave approach.

This report was written by Nick Platten, an independent consultant and formerly an expert at DG 15, the European Commission, Brussels. *Privacy Laws & Business* appreciates the help with this report given by Ms. Evangelia Mitrou, Head of Organisation and Administration, Prime Minister's Office, Greece.