# New Spanish Regulation Tightens Up Data Protection Requirements

RAFI AZIM-KHAN, JOHN NICHOLSON, ALESSANDRO LIOTTA, AND DOMINIC HODGKINSON

*The Spanish government has enacted a new regulation that further develops its data protection legislation by providing additional detail on the security measures required to comply with existing Spanish law. The new regulation came into force on 19 April, 2008, although currently registered businesses have one year to adapt their existing data procedures to the new security measures. While the law is aimed at implementing data security measures and clarifying data transfer issues that arise from the existing data protection legislation, its critics maintain that it merely introduces further regulatory burdens for companies.*

The Spanish Organic Law 15/1999, which implements EU Privacy Directive 95/46/EC, set out the principles that must be applied when processing personal data and established the Spanish Data Protection Agency (Agencia Española de Protección de Datos (AEPD)), which, unlike other European data protection agencies, has strong interpretative, investigative, and prosecutory powers, as well as the authority to impose significant fines on infringing businesses.

---

Rafi Azim-Khan, John L. Nicholson, and Alessandro Liotta, attorneys with Pillsbury Winthrop Shaw Pittman LLP, can be reached at rafi.azimkhan@pillsburylaw.com, john.nicholson@pillsburylaw.com, and alessandro.liotta@pillsburylaw.com, respectively. Dominic Hodgkinson, an attorney in the firm's London office, can be reached at dominic.hodgkinson@pillsburylaw.com.



Published in the May 2008 Privacy & Data Security Law Journal.

The new regulation 1720/2007 provides (among other things) for more specific and tighter security measures, as well as for rules on international data transfers and new applicable requirements and procedures.

## SECURITY MEASURES

The Organic Law currently provides that all data controllers (that is, any individual or legal person who controls and is responsible for the keeping and use of personal information on a computer or in structured manual files) must implement a data processing system based on three security levels: basic, medium, or high. The application of each security level depends on the sensitivity of the data being processed or the nature of the relevant business.

Under the new regulation, the data controller is required to develop and maintain an internal security policy specifying the technical and organizational measures (pursuant to the applicable security level) to be followed by its staff. Where the data processing is outsourced so that the personal data is processed exclusively by the systems of the data processor, the data controller may delegate the obligation to develop and maintain the internal security policy to the data processor.

The new regulation details the measures to be associated with each security level. More specifically:

### A. Basic Security Level

All categories of personal data must be protected, at a minimum, at the "basic" security level, which requires that the data controller must:

- Identify the functions and obligations of the staff having access to the personal data;
- Establish a procedure for the notification and management of all incidents affecting personal data and keep records of such incidents, the notification given, and how such incidents are managed;
- Ensure that its personnel will have access only to that personal data strictly necessary to the performance of their functions;

- Ensure that the devices and documents containing personal data will:
  - Identify the type of data stored; and
  - If they are transferred outside the premises of the data controller, protect against loss or unauthorised access to the data;
- Establish a mechanism allowing the identification of any person trying to access the data; and
- Put in place a disaster recovery system that will include a weekly backup of all the personal data stored.

**B. Medium Security Level**

Data concerning criminal or administrative offenses, solvency status, taxes, financial transactions or status, social security status, or the data subject's personality or behavioral traits, must be protected, at a minimum, at the "medium" security level.

In addition to the measures provided for under the basic security level, the medium level requires that the data controller must:

- Appoint one or more security officers who will coordinate and control the implementation of the measures specified in the internal security policy;
- Undertake internal and external audits;
- Keep records of all receipts and transfers of documents and other media containing personal data;
- Establish a system limiting the possibility of repeated attempts at unauthorised access to the information system;
- Ensure that only authorized personnel have access to the sites where the equipment supporting the information systems is located; and
- Record all the procedures followed for the recovery of data as a result of any incident, including identifying the persons who executed such procedures.

**C. High Security Level**

Sensitive data, including trade union membership, religious or other beliefs, racial origin, health or sex life, data acquired for security forces purposes, and data relating to acts of gender-based violence, must be protected at the "high" security level.

In addition to the measures provided for under the basic and medium security levels, the high level requires that the data controller must:

- Ensure that all media on which data is stored are identified through labels allowing users to identify their content;
- Where the media on which data is stored are transferred, or if personal data is stored on a portable device (e.g., laptops, PDAs, USB drives, or other portable memory devices) and such device is located in a place that is outside the control of the data controller, ensure that the data is encrypted or otherwise protected so that it cannot be accessed or manipulated by unauthorised individuals;
- Maintain a backup copy of the data in a different place from the location where the data is processed;
- Keep a record (for at least two years) of any attempt to access the data, identifying:
  - The user, the date and time of the attempt;
  - The data accessed;
  - The type of access; and
  - Whether the attempt was authorized or denied;
- Ensure that the security officer reviews the access register at least once a month; and
- Ensure that the transfer of personal data through public networks or wireless electronic communications networks is encrypted or otherwise protected to ensure that such data cannot be accessed or manipulated by unauthorized individuals.

To facilitate compliance with the applicable security measures, soft-

ware products to be used in the processing of personal data shall include, in their technical description, the security level (basic, medium, or high) that they can meet.

## SECURITY AUDIT

For medium and high security level data processing, the new regulations specify that all data processing systems must be subject to an internal or external audit at least every two years to verify compliance with the applicable security level requirements.

A further audit must be carried out every time substantial changes are made to the processing system that could affect the security measures for medium and high security data. For example, if a data processing function is being outsourced to a service provider, where the outsourced service provider is expected to change the information system or transfer the data processing function offshore, an audit must be performed.

Following each audit, a report must be prepared specifying the security measures applied and identifying any further measures to be undertaken to comply with the regulation. The audit reports must be given to the data controller's security officer, who will keep them and provide them to the AEPD upon request.

## INTERNATIONAL TRANSFERS

The new regulation further sets out the procedure to follow prior to an international transfer of data to countries outside the European Economic Area ("EEA") that are not considered as providing an adequate level of protection.

There are several ways for such an international transfer to be authorized: consent of the data subject, use of the Model Contractual Clauses ("MCC") (as approved by the European Commission Decisions 2001/497, 2002/16 and 2004/915), or implementation of an alternative data protection regime. Unless the data subject consents to the international transfer, the data exporter and the data importer must either enter into the MCC or an alternative written contract containing adequate data security measures. If the parties decide to enter into an alternative

arrangement (including, in the case of intracompany or intracorporate group transfers, the implementation of Binding Corporate Rules ("BCR")), then the transfer will be subject to prior authorization by the AEPD as described below.

The procedure to obtain AEPD authorization must be initiated by the data exporter by depositing a copy of the contract or the BCR with the AEPD. The Director of the AEPD will, within three months of the application, adopt a resolution either authorizing or rejecting the transfer. If, at the end of the three months, the Director of the AEPD has not adopted any resolution, the transfer will be deemed authorized.

At any time (even when authorization has been given), the Director of the AEPD may, following a hearing with the data exporter, temporarily suspend the transfer, where:

- The protection of fundamental rights and civil liberties in the country of destination or that country's legislation, does not guarantee the data importer's compliance (or ability to comply) with the provisions of the contract;
- The data importer has previously breached guarantees similar to those provided for in the contract;
- There are reasonable indications that the data importer will not comply with the guarantees provided for in the contract;
- There are reasonable indications that the measures provided for in the contract will not be effective; or
- The transfer, or its continuation if it has started, may create a risk situation for the data subject.

## CONCLUSION

The Spanish data protection regime has long been considered one of the more cumbersome Member State regimes.

Data controllers and data processors subject to Spanish privacy regulations will find the new regulations useful in clarifying several issues that were previously left to the interpretation of the AEPD and the Span-

ish courts. However, as some Spanish commentators have written, there is also a good chance that businesses may feel overregulated, especially considering the risk of fines that can be as high as 600,000 euros.

The cost that businesses will incur to comply with the new regulations are yet to be proven, but they may be onerous — particularly with regard to the security measures and the audit requirements. The international transfer procedures and the powers given to the Director of the AEPD in relation to such transfers may also have an impact on transfer costs and timeframes.

In particular, when an entity controlling data pertaining to Spanish data subjects is considering entering into an outsourcing contract, careful attention should be paid to the applicability of Spanish regulations and the impact that any costs, procedures, and timeframes may have on the overall outsourced solution.