



AUDITING AND ENFORCEMENT AT THE SPANISH DPA. EXPERIENCE WITH OUTSOURCING TO COUNTRIES WITH A NON ADEQUATE LEVEL OF PROTECTION

CONFERENCE ON CROSS-BORDER DATA FLOW & PRIVACY

October 15 – 16, 2007

Washington, D.C., USA

Workshop on The European Union's Data Protection Framework – 12 Years Later

Tuesday, October 16, 2007

10:45 – 12:45 am

Dr. Artemi Rallo Lombarte
Director, Spanish Data Protection Agency

- **Unprecedented enforcement action outside the EU: onsite inspections of data transferred to Colombia.**
 - Performance of an ex officio sector inspection of data importers who receive previously authorized international data transfers at call centers established in third countries which do not ensure an adequate level of protection.
 - **Purpose:** verify effective compliance with the Spanish Data Protection Law at customer telephone attention centers established by companies in the telecommunications sector in and out of the national territory.

- **Why we carried out an ex officio sector inspection in Colombia (I):**

- The amount of cross-border flow of personal data between different public and private agents established in different countries has increased in recent years.
- Up to the 1st July 2007, 8,483 international data transfers were reported to the General Data Protection Registry.
- The main countries of destination are the USA (87 authorizations since 2000) and, from last year, Latin American countries (Chile, Peru and Colombia) and Morocco.
- The 58% of the authorizations granted by the Agency are related to multinational groups which have their parent company outside of Spain, mainly in the USA, and their activity spread through many countries (for example, one may mention global personnel management by international companies).
- Up to 2004 there were no authorizations to Latin America. From 2005 uptill now, 35 transfers of data have been authorized to these countries.

- **Why we carried out an ex officio sector inspection in Colombia (II):**
 - Many Spanish companies adopt global sourcing to third countries, specially to Latin American countries.
 - Different Spanish Trade Unions, aware that data might be at risk of misuse or vulnerable to security breaches, communicate their worries to the Spanish DPA.
 - The Spanish DPA took the decision to audit onsite certain data importers .
 - It was considered necessary not only to evaluate the legal sufficiency of the guarantees provided by the applicants and their effective fulfillment, but also to analyze the transfer procedure.

- **Selection of the sample:**
 - **Why the telecommunication sector:**
 - The Spanish DPA had received certain concern over this processing from different Spanish Trade Unions.
 - Spanish telecom companies have global sourcing for their services in Latin America.
 - In May 2007, the whole telecom sector had a total of 22 international transfer authorizations, representing a 15% of the whole amount of authorizations.
 - Two operators in the telecom sector, which offer operation of the commercial telephone care services, break down care services and telemarketing, in relation to the fixed telephony and internet services, were investigated.
 - These two operators hold a market share of 80% of the Spanish market.
 - **Why this purpose:**
 - The 22% of these authorizations refers to customer care or telemarketing services by data importers established in Latin America (mostly in Chile, Peru and Colombia).

- **Legal framework for transfers of personal data to third countries:**
 - Countries considered by the European Commission to have an **adequate standard of protection** pursuant to Directive 95/46/CE: countries parties to the Agreement on the European Economic Area, Switzerland, Argentina, Guernsey, Isle of Mann, Canada (with regards entities subject to application of the Canadian Personal Information Protection and Electronic Document Act) and the USA (with regard to firms that have adhered to the “Safe Harbor” principles).
 - Countries which do not ensure an adequate level of protection, but which are covered by the **derogations** of the Article 26 Directive 95/46/CE (among others, application of treaties or conventions to which Spain is a party, to provide or request international judicial assistance, when necessary for performance of a contract between the data subject or the controller...)
 - **Authorization by the Spanish DPA Director**
 - Third countries.
 - Section 33.2 LOPD: Adequate guarantees: **standard contractual clauses** for international data transfers between data importer and exporter in order to warrant that they have complied with data protection standards which meet the requirements of the Data Protection Directive in respect of the data.

- **Legal basis for transfers of personal data to third countries (I):**
 - In this particular case, as the **transfer of personal data took place to a country with a non adequate level of protection, as Colombia**, it had to be based on the Commission Decision 2002/16/EC. Because of that, a **written contract entered into between the data exporter and the data importer**.
 - **Telecom companies included these contractual clauses in contracts signed with the companies acting as the processors for Colombian technical support outsourcing.**
 - Where data is transferred internationally, **the DPA may conduct audits of the importer**, using the same techniques and tools that are available for audits of the exporter in the DPA's jurisdiction.

- **Legal basis for transfers of personal data to third countries (II):**
 - Spanish Telecom companies (controllers) outsource their customer services (or telemarketing) to other companies specialized in this area (processors) in third countries.
 - These processors can be:
 - Spanish firms with branches in a third country
 - Or, third countries companies specialized located only in these third countries.

• Methodology : three phases (I)

- The methodology used is based on identification of the purposes of the transfers and development of a plan of action in three phases.

- First phase**: Physical visits in Spain to the telecom operators (controllers) in order to:

- Analyze and specify the services provided from companies located in Colombia.
- Audit the processing of personal data.
- Check the information accessed is adequate.
- Study the security measures implemented for access to the personal data.

- **Methodology : three phases (II)**

- **Second Phase**: Inspections in Spain have been performed by the processor who has a head office in Spain and a branch in Colombia.

- Analysis of the services provided from the offices located in Spain and from those located in Colombia, as well as the data flows between both;
- Checking compliance of the processing performed by these entities with the purposes recorded in the service provision agreements;
- Studying the security measures implemented for access to the personal data.

- **Third phase**: Visits in Colombia to processors located there, with collaboration by the telecom operator (controller).

- **Cooperation by exporter (data controller)**
 - Coordinating inspections
 - Contact point for audits
 - Auditing all data importers involved in Colombia

- **5 days of auditing in Colombia**
 - 3 inspectors + The Inspection Head Deputy
 - Document access and examination
 - *Onsite* checks of technical systems
 - Access to and evaluation of stored information.
 - *Onsite* verification of security measures

- **Conclusions of the inspection (I):**
 - **Findings:** general compliance with technical and organizational security requirements.
 - **Processing the audited data:**
 - The data processing matches the services specified in the contract provided in the application for the international transfer authorized by the Spanish DPA.
 - The personal data to which the processor companies have access is considered necessary to provide the contractual services.
 - Under no circumstances should there be transfer of the telecommunications files to the companies that act as a processor.

- **Conclusions of the inspection (II):**
 - **Security measures:**
 - Measures adopted by the controllers:
 - The telecom operators adopted measures to protect the information contained in their files.
 - The confidentiality of access to the information is guaranteed by setting up an encrypted channel between ends.
 - Measures adopted by the processors:
 - Suppression of the peripheral devices that allow information to be extracted at all the work stations.
 - No computer applications have been installed that provide print screen functions or document printing facilities.
 - Identification and authentication of telephone operators located in Colombia.

• Recommendations:

- Level of security
- Access through networks
- Identification and authentication
- Staff duties and obligations
- Auditing
- Data access terminals
- Duty of confidentiality.
- Conclusion of a contract between data exporter and importer.
- Information to the Workers' Committee of the controller telecom company.
- Publication in the Spanish Official Journal.



AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

