AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

SPANISH DATA PROTECTION AGENCY

REPORT ON INTERNATIONAL DATA TRANSFERS

EX OFFICIO SECTORIAL INSPECTION OF SPAIN– COLOMBIA AT CALL CENTRES

JULY 2007

INDEX

I. BACKGROUND & PRESENT SITUATION

II. *EX OFFICIO* SECTORIAL INSPECTION SPAIN-COLOMBIA IN THE CALL CENTRE SECTOR

1 INSPECTION METHODOLOGY

A SELECTION OF THE INSPECTION SAMPLE

B PHASES OF THE ACTIONS

C PROCESSING THE DATA CHECKED

D TECHNOLOGICAL ENVIRONMENT

2 CONCLUSIONS OF THE INSPECTION

A PROCESSING THE DATA AUDITED

B SECURITY MEASURES

III. PROCEDURAL NOVELTIES

1 PUBLIC INFORMATION

2 CONFIDENTIALITY OF THE FILE DOCUMENTATION

3 FULFILMENT OF OTHER LEGAL OBLIGATIONS

IV. RECOMMENDATIONS

1 *EX OFFICIO* SECTORIAL INSPECTION SPAIN - COLOMBIA IN THE CALL CENTRE SECTOR

2 AUTHORISATION PROCEDURE

3 APPLICATION VERIFICATION INDICATORS

ANNEX. REGULATORY FRAMEWORK

The object of this paper is to describe the regulatory framework that is to be taken into account to perform international transfers of personal data, as well as to show the way to apply for the required authorisation by the Director of the Spanish Data Protection Agency in cases in which it is foreseen to transfer personal data to countries that do not provide an adequate level of protection, when that transfer is not covered by any exception foreseen under Article 34 of the Spanish Organic Act on Data Protection (LOPD).

Throughout the document, mention is made of the initiatives adopted by the Spanish Data Protection Agency in order to audit the existing practices in the Call Centre sector, within the scope of telecommunications operators, and to provide greater transparency and guarantees in the international data transfer authorisation procedure. The recommendations prepared based on these initiatives are also recorded.

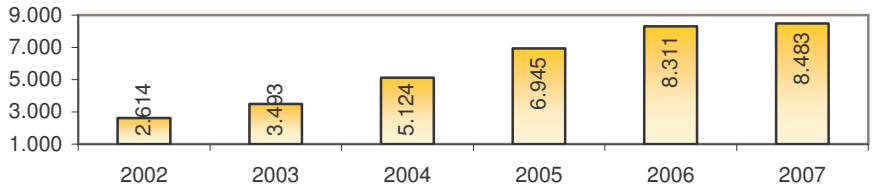
I BACKGROUND & PRESENT SITUATION

The economic and social integration arising from establishment and operation of a globalised market has involved a notable development of cross-border flows of personal data between different public and private agents established in different countries. Such data flow has been favoured by factors such as progress of information technologies and, in particular, the development of the Internet, that considerably facilitate information processing and exchange, and which allow technological resources to be shared, to centralise certain activities and processes and cheapen costs of services provided by the business concern outside the country where it is established.

The Spanish Data Protection Agency has been able to notice this considerable increase in international data transfers through notification of files registered at the General Data Protection Register, where 8,483 transfers had been declared on 1 July 2007.

This figure includes communications of data notified to the Register with a destination in countries parties to the Agreement on the European Economic Area and those that have been considered by the European Commission to have an adequate standard of protection pursuant to Directive 95/46/EC, which is the case of Switzerland, Argentina, Guernsey and Isle of Man, as well as Canada, with regard to entities subject to application of the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), and the United States, with regard to firms that have adhered to the “Safe Harbour” principles. It also includes those that, while not having a country with an adequate standard of protection as their destination, are covered by the exceptions foreseen in Article 34 of Spanish Organic Act 15/1999, of 13 December, on Personal Data Protection and, lastly, by the 149 that have needed authorisation from the Director of the Agency.

Evolution of international data transfers notified at the Register.
1 July 2007



Authorisations of international transfers. 1 July 2007[1]

	2000	2001	2002	2003	2004	2005	2006	2007		Total Authorisations
								Authorisations	Other applications	
USA	1	9	2	6	40	9	16	4	4	**87**
Morocco	1	-	-	-	2	2	2	1		7
India	-	-	-	-	4	-	3		1	7
Singapore	-	-	-	-	1	-	1		1	2
Japan	-	-	-	-	-	1	-		1	**1**
Panama	-	-	-	-	-	2	-			**2**
Colombia	-	-	-	-	-	1	4	2	3	7
Malaysia	-	-	-	-	-	1	1		1	2
Thailand	-	-	-	-	-	1	-		1	1
Chile	-	-	-	-	-	1	7	7	1	**15**
Uruguay	-	-	-	-	-	1	1		2	**2**
Philippines	-	-	-	-	-	-	3	1		4
Peru	-	-	-	-	-	-	4	3	3	**7**
China	-	-	-	-	-	-	1		1	1
Hong Kong	-	-	-	-	-	-	1			1
Guatemala	-	-	-	-	-	-	1			**1**
Paraguay							1		1	**1**
Australia									1	
Brazil									1	
Canada									1	
Egypt									1	
El Salvador									1	
Nicaragua									1	
Nigeria									1	
Applications submitted	2	9	2	19	56	45	54	49		236
Archived / in process	-	-	-	13	6	16	17		36	88
Authorisations	2	9	2	6	47	19	46	18		148

With regard to the purposes for which these international transfers for which authorisation by the Director of the Agency are requested are performed, one may state:

- Purposes related to the internal needs of **corporate management in a global context**. Multinationals need to perform international data transfers for such purposes as management, maintenance and technical support for information systems. On the other hand, these authorisations are requested in relation to the efficient management of human resources, customers and providers, as well as providing administrative support services in relation to these.

This category of international transfers amounts to 58% of the authorisations granted by the Agency, that are related to multinational groups which have their parent company

[1] This data refers exclusively to transfers that require authorisation by the Director, due to their destination being countries that do not have an adequate standard of protection. It is necessary to bear in mind that there are authorisations that have more than one receiver, located in different countries. Likewise, some applications for authorisation have been resolved in the year following their submission.

outside of Spain, mainly in the **United States of America**, and their corporate activity spread throughout many countries. For example, one may mention global personnel management by international companies.

- Telephone care for customer and other telephone marketing actions intended to improve their degree of satisfaction, as well as centralised management of call centres.

This group mainly includes provision of **customer care or telemarketing services** by data importers established in **Latin America**, that have significantly increased in the last two years and amount to 22% of the authorisations by the Agency.

In relation to such authorisations, the Agency has been able to record the existence of certain concern over this processing. At different meetings with representatives of Trade Unions, it has noted the existence of persons or groups who hold legitimate rights or interests that might be affected by the relevant authorisation resolutions.

Bearing these issues in mind, the Agency has considered it necessary not only to evaluate the legal sufficiency of the guarantees provided by the applicants, but also their effective fulfilment. Moreover, an attempt has been made to provide greater transparency to the authorisation procedure, for which the following initiatives have been adopted:

- Performance of an ***ex officio*** **sectorial inspection** of certain data importers who receive previously authorised international data transfers at call centres established in third countries.
- Introduction of public information formalities in processing the procedures for which authorisation is required by the Director of the Spanish Data Protection Agency, pursuant to Article 33.1 of Spanish Organic Act 15/1999.

II. *EX OFFICIO* SECTORIAL INSPECTION SPAIN – COLOMBIA IN THE CALL CENTRE SECTOR

The Spain - Colombia *ex officio* sectorial inspection was intended to verify effective compliance with

Spanish Organic Act 15/1999 and its implementation regulations at customer telephone attention centres established by companies in the telecommunications sector, concluding with formulation by the Director of the Agency of a series of Recommendations aimed at improving practices in the sector in relation to data protection.

1 . INSPECTION METHODOLOGY

A. SELECTION OF THE INSPECTION SAMPLE

The selection of the sample to inspect was performed in May 2007. On that date, the whole telecommunications sector had a total 22 international transfer authorisations recorded on the General Data Protection Register, with the exception of those that had the United States of America as their destination. With the exception of 3 authorised transfers with Morocco as their destination, the rest have Latin American countries as their destination, mostly Chile, Peru, Colombia and, to a lesser extent, Guatemala, Uruguay and Panama.

To determine the selection, the Agency also applied criteria based on the market shares published by the Telecommunications Market Commission, and the social concern shown in diverse media in relation to customer data transfer from this operator to the Republic of Colombia.

FUENTE: CMT Obtenido de Red.es Observatorio Julio 2006

Market shares by total service revenue: basic land lines

Market shares by total service revenue: automatic mobile telephony

…. Rest … Rest of Cable operators

SOURCE: CMT Obtained from Red.es Observatory July 2006

The applications for international data transfer made under Article 33 of Organic Act 15/1999 on Protection of Personal Data, when the service provider is established in countries not declared to have a comparable protection level, are usually based on fulfilment of the guarantees specified in Decision by the Commission 2002/16/EC. These must be embodied in a written contract, entered into between the data exporter and importer, recording the necessary guarantees of compliance with protection of the private life of the parties affected and their fundamental rights and liberties and guaranteeing exercise of their respective rights.

In the case of Colombia, the contracts signed between the telecommunications operators and the companies acting as processors include a clause that specifies the agreement by all parties that the Spanish Data Protection Agency is empowered to audit the importer to the same extend and under the same conditions as it would do with regard to the data exporter under the Spanish laws in force in matters of data protection. Moreover, it stipulates that the data importer warrants that, at the request of the exporter and/or Agency, it shall make its data processing facilities available to the latter to carry out the audits deemed appropriate.

B. PHASES OF THE ACTIONS

The data inspection has concentrated its investigations on international transfers of authorised data in two operators in the telecommunications sector, which offer operation of the commercial telephone care service, breakdown care service and telemarketing, in relation to the fixed telephony and the Internet services for residential customers, as well as mobile telephony for the freelance and small and medium sized businesses sector.

The methodology used is based on identification of the purposes of the transfers and development of a plan of action in three phases consisting of performing physical visits to those responsible for files in Spain, inspecting those in charge of treatment with offices in both countries and auditing those in charge of processing located in Colombia.

The first phase of physical visits to the telecommunications operator premises covered the following objectives:

- Analysis and specification of the services provided from companies located in Colombia;
- Auditing the processing of personal data, and obtaining information on accesses performed from Spain and from Colombia;
- Checking that the information accessed is adequate for what is established in provision of the contractual service;
- Studying the security measures implemented for access to the personal data performed from Spain and from the entities located in Colombia;
- Evaluation of the technological environment used for international data transfer.

In a second phase, inspections have been performed of the processors that have a head office in Spain and a branch in Colombia. These actions have concentrated on the following aspects:

- 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;
- Checking the personal data accessed at these firms and verifying whether they are relevant in relation to the services established;
- Verifying the security measurements implemented in relation to the instructions established by the person responsible for the file and their adaptation to what is set

forth in Royal Decree 994/1999 of 11 June, that approves the Regulations on Security Measures of automated files that contain personal data;

- Evaluation of the technological environment used for access to personal data, as well as in charge of processing by the telecommunications operator.

In a last phase, visits have been made to processors located in Colombia, with collaboration by the telecommunications operators responsible for the files. Two different cases have been detected in this phase, that have given rise to two ways of acting:

On one hand, in the case of Spanish firms with a branch in Colombia, the visit was approached as an inspection performed on the premises of the firm acting as processor, in order to compare what was already verified at the Spanish head office, with emphasis on the most relevant aspects according to the place from which the service is provided. In performing these actions, collaboration by the controller and processors located both in Spain as well as Colombia was available at all times.

On the other hand, the physical visits performed by the Subdirector General of Data Inspection and three Data Inspectors from the Agency to the processors with offices in Colombia alone, involved requiring the telecommunications operator being the controller, at the request of the Data Inspectors and in close collaboration with them, to provide all the information and documentation and to allow access to the necessary information systems to be able to perform the audit, using the resources implemented at the firm in Colombia.

In both cases, the objectives intended by the actions have been:

- To check the adequacy of the processing performed by these entities against the purposes recorded in the service provision contracts;
- To check the personal data accessed from these firms and to verify that they are pertinent in relation to the services established;
- To verify the security measures implemented in relation to the instructions established by the controller and their compliance with what is set forth in those Security Measures Regulations;

- To evaluate the technological environment used for access to personal data, as processor for the telecommunications operator.

C. PROCESSING THE DATA CHECKED

The processing performed by the firms hired is performed to provide the telecommunications operators the following services:

- Operation of the commercial telephone care service for residential customers. Customer calls are received and made from Colombia, with data processing related to information on deliveries pending and billing, and incidents and complaints concerning these. Moreover, at the request of the customer, personal data may be gathered to register new telephone lines.
- Operation of the commercial telephone service for freelance and small and medium sized business customers. The service performed consists of data processing for administrative management and incident solving, verification of the documentation provided in applications for registration, removal from contractual services and issue of calls when it is necessary to inform the customer.
- Telemarketing Services for customers of the operator. Telephone contact is made with the customers to offer the product and, if appropriate, to record it in the actual Information System of the person responsible at the same time.

D. TECHNOLOGICAL ENVIRONMENT

With regard to the technological structure for delocalisation of the services, in the case of the Spanish company providing the services with a branch in Colombia, two optic fibre links are used, connected directly to offices of the company located in Spain, that in turn are linked to the corporate network of the telecommunications operator. This allows the users working from Colombia access to the same services and resources as those doing so from the local area network of the Spanish centres. For greater security, the communications connections architecture mentioned uses an encryption system for all processes involving personal data.

With regard to the company that provides services, which has its offices in Colombia alone, the technological structure for delocalisation is based on leased lines, owned by the operator that has commissioned provision of the service giving rise to the international transfer. In this case, there are two dedicated lines, by submarine cable, linked directly to the operator's trunk network. Administration of the communications network devices is performed by the operator's staff.

To date, the audits and controls performed by the controllers have not detected any incident.

2 .CONCLUSIONS OF THE INSPECTION

A. PROCESSING THE DATA AUDITED

The data processing matches the services specified in the contracts provided in the application for the international transfers authorised by the Spanish Data Protection Agency.

The personal data to which the processor companies have access are considered those necessary to provide the contractual services.

Access to personal data is performed directly on the Information Systems and files of the parties responsible located in national territory and regardless of the geographic location of the processor.

Under no circumstance is there transferral of the telecommunications operator files to the companies that act as a processor.

The services now performed may be modified – added to or suppressed – at all times as, just as stated, they use the Operator's own information systems.

Under criteria of quality, service and cost, all the telephony operators inspected shortly foresee an increase in delocalised services that require access to their customer data from third countries, or the percentage of operations performed from Colombia.

B . SECURITY MEASURES

Measures adopted by the controllers:

- The telecommunications operators have adopted diverse measures to protect the information contained in their files, among others, not allowing mirroring of files with personal data outside the Spanish territory, using dedicated communications lines for access from Colombia and having logical security devices implemented.
- The confidentiality of access to the information is established by setting up an encrypted channel between ends, although it has been detected that this measure has not been implemented with regard to all the data flows.
- The accesses performed by telephone operators located both in Spain as well as in Colombia are shown in the telecommunications Information Systems operators audited.

Measures adopted by the processors:

- According to instructions from the controllers, service providers located in Colombia have suppressed the peripheral devices that allow information to be extracted at all the work stations used by the telephone operators.
- No computer applications have been installed that provide print screen functions or document printing facilities.
- Identification and authentication of telephone operators located in Colombia with access to the operator's files containing personal data are performed by user code and password through a tool owned by the controller that manages assignment of passwords and the data access profiles.

III PROCEDURAL NOVELTIES

As previously emphasised, a public information formality has been included in the international data transfer authorisation procedure.

This formality aims to provide the procedure greater transparency and guarantee intervention in it by those who consider it convenient to make allegations. Notwithstanding this publicity, one must bear in mind the confidentiality guarantee with regard to certain data in the file.

Lastly, one must point out that certain transfers require prior information to be submitted to the company committee under their specific regulations.

1. PUBLIC INFORMATION

Inclusion of this formality in the international data transfer authorisation procedure can be deemed included in the general provisions contained in Article 86 of Spanish Act 30/1992, of 26 November, on the Legal Regime of the Public Administrations and the Common Administrative Procedure (LRJPAC).

In this sense, due to the term for public information established in Article 86.1 of the LRJPAC being 20 days, which makes it difficult for the Agency to process the file within the

legally established term, a proposal has been made to introduce application of Article 86.4 to reduce the public information term to 10 days in the **Draft Regulations** for the implementation of the LOPD.

2. CONFIDENTIALITY OF THE FILE DOCUMENTATION

Considering that the documentation shall be subject to public information, the exporter may indicate its degree of confidentiality, whether it is affected by commercial secret under the terms provided in Article 37.5 of Act 30/1992, on Administrative Procedure (LRJAP). In any case, the general contractual clauses that regulate the transfer and its description may be submitted to public information.

3. FULFILMENT OF OTHER LEGAL OBLIGATIONS

As a prior condition to performing the international data transfer, the data exporter must fulfil the rest of the obligations established in the data protection regulations, and any others that might be applicable.

A paradigmatic case arises when data transfer may affect other workers' rights. In this case, one must bear in mind fulfilment of the obligations related to Labour Law and, in particular, the obligation to inform the **company committee** pursuant to Article 42.4 of the Workers' Statute (Legislative Royal Decree 1/1995, of 24 March) in relation to transposal of Directive 2002/14/EC, of the European Parliament and of the Council, establishing a general framework for informing and consulting employees in the European Community.

IV. RECOMMENDATIONS

1. *EX OFFICIO* SECTORIAL INSPECTION SPAIN – COLOMBIA IN THE CALL CENTRE SECTOR

From the result of the proceedings conducted by the Data Inspectors at the companies that perform international data transfers to provide services related to Call Centres, one may conclude that the most relevant aspect to be taken into account concerns the **safety measures** of the Information Systems that allow access to guarantee the confidentiality and integrity of customer data.

Due to this, the Director of the Data Protection Agency, by virtue of the powers he is granted under Article 5 c) and d) of Royal Decree 428/1993, of 26 March, that approves the Statute of the Agency, provides the following **RECOMMENDATIONS** to be observed by firms in order to adapt automated processing they perform to the principles of the regulations in force on matters of personal data protection.

ONE: In relation to Personal Data Security. (Article 9 of the LOPD and Royal Decree 994/1999)

Royal Decree 994/1999, of 11 June 1999, approves the Regulations on Security Measures for automated files that contain personal data, which are classified on three levels, according to the nature of the information processed and the greater or lesser need to guarantee the confidentiality and integrity of the information.

a) Security level.

According to the terms established in those Regulations, entities must comply with the security measures applicable to each one of the files according to their classification.

In cases that allow evaluation of the citizen's personality, adoption of medium level security measures must be guaranteed with regard to it being obligatory to perform a biannual audit of fulfilment of the Security Regulations, to establish a mechanism to allow unequivocal, customised identification of all users who attempt to access the Information System and verification that they are authorised; to establish adequate physical access controls, as well as establish an input and output register of media containing personal data.

b) Access through networks

Access to personal data through the telecommunications networks must be performed with security measures that guarantee an equivalent security level to that of accesses in local mode, fulfilling the terms of the Security Measures Regulation in each case, according to the nature of the data accessed. Due to this, it is considered good practice, in cases in which it is not required by the regulations, as verified at the companies inspected, to use secure physical channels, either through owned or dedicated lines, avoiding the use of the public telecommunications networks wherever possible. In cases of use of public networks, it is recommendable to use secure logical channels, using protocols that allow information to be encrypted.

c) Identification and Authentication

Article 11 of those Regulations also specify that when the authentication mechanism is based on the existence of passwords, there shall be an assignment, distribution and storage procedure for these to guarantee their confidentiality and integrity. Those passwords must periodically be changed and stored in an unintelligible manner.

On the other hand, Article 18 of those Regulations specify that users who access personal data must be unequivocally and personally identified, verifying that they are authorised for that access. Likewise, the possibility of repeatedly attempting non-authorised access to the information system must be limited.

It is advisable to precisely define the profiles for access to the Information Systems, in order to guarantee that the users have access only to the necessary features for the work they perform.

It is also convenient to use an integral user code and password management system, managed and controlled directly by the controller, establishing identification and authentication mechanisms so identification of the user attempting to access the system is unequivocal and personalised and guarantees the confidentiality and integrity of the passwords. A password distribution system must also be used to assure their confidentiality.

d) Staff duties and obligations

As specified in Article 9 of the Regulations on Security Measures, the functions and obligations of each one of the persons with access to personal data and the Information Systems must be clearly defined and documented, and the controller must take the necessary measures so all the staff know their duties and obligations, as well as the

security rules that affect their performance and the consequences arising from their infringement.

Thus, the controller must require the importer to adopt the appropriate measures to inform all its members of staff of the Spanish data protection law applicable to them.

e) Recording incidents

As specified in Article 10 and, when appropriate 21 of the Security Measures Regulations, an Incident Record must be established, including the anomalies that affect or might affect the security of the data and containing at least: type of incident, date and time when it took place, person performing the notification, person notified and effects arising.

In this regard, it would be recommendable for the controller to have knowledge of the incidents in security matters that arise at the importer and related to access to the data giving rise to the transfer.

f) Auditing

Article 17 of the Security Measures Regulations makes it necessary to perform internal or external security auditing to verify fulfilment of those Regulations and of the procedures and instructions in force on matters of data security, at least every two years. The auditing report must be performed by the competent security manager, issuing a report on compliance with the measures and controls with the Regulations, identifying deficiencies and proposing the necessary corrective or complementary measures to be adopted by the controller.

To that end, it is considered good practice, in cases when not required by the regulations, for these audits to be performed by the controller, for all processing performed by importers of personal data, regardless of their nature. In all cases, the controller shall notify the importer of the conclusions in order for him to adopt the appropriate corrective measures, control of which must be performed by the controller.

g) Data access terminals

For greater security, it is recommended that delocalised work stations have the peripheral devices through which information may be extracted disabled, as well as eliminating procedures that facilitate data capture, having only the applications required to provide the service.

Access to Internet shall be limited to the work stations where it is strictly necessary.

TWO: In relation obtain data access on behalf of third parties (Article 12 of the LOPD).

With regard to provision of services

Likewise, as in the case of the firms inspected, the exporter and importer must sign a service provision agreement, under the terms provided in Article 12 of the LOPD.

To these ends, it is recommended that, in provision of services aimed at performing data processing on behalf of a third party, the firm must bear in mind, as controller, that the service must be recorded in a contract that must in writing, and it shall specifically establish that the receiver shall only process the data according to instructions given by the transmitter, that it shall not apply or use them for purposes other than those recorded in that contract and that it shall adopt the security measures required of the conveyor according to the Spanish data protection regulations.

Moreover, it must indicate that, once the contractual service is fulfilled, the personal data must be destroyed or returned to the transmitter, as must any media or document containing any personal data subject to processing.

In the cases analysed, access to the data by companies located in third countries is performed by telematic means, through computer applications provided by the controller, so in principle there is no possibility of obtaining a copy of the data on media or in documents.

In any case, the receiver may not communicate the data to other parties, not even for conservation.

THREE: In relation to the duty of secrecy (Article 10 of the LOPD).

The companies must adopt the appropriate measures to ensure the workers are informed of the requirements in security matters and the obligation and duty of secrecy. In this regard, it is considered good practice for the workers to sign a document informing them of those terms.

It is recommended for labour contracts to include clauses concerning the duty of secrecy with regard to personal data the employees have access to due to their activity, either the

actual employee of the firm, as well as the employees of the firms providing services to the entity with access to customer personal data.

2 . AUTHORISATION PROCEDURE

Processing the authorisation procedure for international data transfers and inclusion of a public information formality must be adapted to the legally established processing term established for the Agency to resolve these files. Due to this, it is highly important to take absolute care when submitting the appropriate documentation, in order to expedite processing.

To that end, the following recommendations must be taken into account:

ONE. Fulfilment of prior obligations.

The controller who applies for an international data transfer authorisation is obliged to fulfil the rest of the obligations established in Organic Act 15/1999 to perform the relevant data processing in Spain.

Among others, he must have fulfilled the obligation to notify the files concerned to the General Data Protection Register and to keep the information of that inscription up to date.

On the other hand, he must fulfil any other legal obligation related to the object of the international transfer. Among these, if appropriate he must have informed the Company Committee under the terms provided in the Workers' Statute.

TWO. Requisites of the application

In its application to the Agency, the exporter must provide:

- The identification of the file or files whose data are subject to international transfer, stating its name and the inscription code/s on the General Data Protection Register;
- The transfer or transfers for which the authorisation is requested, with a description of the purpose that justifies it and the basic processing operations associated with it, as well as a detailed description of the personal data of the file or files, stated in the preceding point, that are subject to transfer;

- The documentation that includes the guarantees required to obtain the authorisation that must record a description of the specific security measures that are to be adopted, both by the exporter as well as by the importer of the data, during their transfer and in relation to the file or files subject to same;
- An authenticated copy of the contract between exporter and importer of the data, also accrediting that the parties granting have sufficient powers;
- To facilitate the valuation of the application, it may also be of interest to provide any other information that might contribute to clarify in which situations information flows are to take place, indicating the technological infrastructure to be used, specifying whether it is remote access, or by sending media, or any other relevant data.

THREE. Standard contractual clauses

The Decisions by the Commission, adopted as provided under Directive 95/46/EC of the European Parliament and the Council, are now as follows:

- Commission Decision 2001/497/EC, of 15 June 2001, on standard contractual clauses for the transfer of personal data to third countries;
- Commission Decision 2002/16/EC, of 27 December 2001, on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC;
- Commission Decision 2004/915/EC, of 27 December 2004, amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries.

In the event of the transfer being covered by any of these Decisions, the contract between the exporter and importer must include those contractual clauses prepared by the Commission, adapted to the specific situation of the transfer for which the authorisation is requested, not being limited to a literal transcription, but rather, developing the examples stated in the Decisions and, including the following in all cases.

- The identifying data of the data exporter and importer;
- Details of the transfer, in particular the special categories of personal data;
- Clauses of specific third party beneficiaries which the parties concerned may require of the data exporter and importer;
- The obligations of the data exporter;

- The obligations of the data importer;
- Liability for damage caused to the data subjects;
- Mediation and jurisdiction;
- Co-operation with the controlling authorities;
- Applicable legislation;
- Variation of the contract; and
- Obligations once provision of the services has ended.

FOUR. Formalisation terms

The carrying out of the proceedings makes it advisable for the applicant to collaborate diligently, to which end it is most convenient to know its formalities and terms, and to answer requests by the Agency as soon as possible.

Specifically, it is recommendable for the controller to be particularly diligent in responding to the allegations presented in the public information formalities, especially when it is not going to raise any other allegation. In that case, it must inform the Agency of that fact in writing, as that allows it to conclude the formalities and expedite the proceedings.

FIVE. Binding Corporate Rules

An alternative model to fulfil the requisites to allow international transfers to be authorised consists of setting Binding Corporate Rules (BCR). This model is usually considered in the case of international groups and is reasonably complex to formalise.

When a company or group of international companies opts for that means, it must previously assess its convenience, on the basis of the working documents of the Article 29 Working Party: WP 107, WP 108 and WP 74, that explain, respectively, the co-operation procedure to issue common findings on binding corporate rules, the checklist to request approval of BCR's and application of Article 26.2 of Directive 95/46/EC, to the Binding Corporate Rules for international data transfers.

3. APPLICATION VERIFICATION INDICATORS

In order to establish the adequate balance between the guarantees required of the applicants, along with agility in processing the international transfer authorisation files, the following is a list of the control indicators that may be taken into account when requesting authorisation and that are intended to provide help in establishing the existence of an adequate control environment with regard to personal data processing.

SOLE. List of indicators to verify the authorisation application.

Before proceeding to request an international data transfer authorisation, it is recommended to verify the following particulars in order to speed up its processing:

- Has the data exporter filed a specific application for authorisation of international transfers?
- Have the file or files whose data the international transfer concerns been identified, stating under whose name and inscription codes at the RGPD?
- Has the purpose that justifies the transfer being described?
- Have the basic processing operations related to the purpose of the transfer been described?
- Have the personal data to be subject to transfer been described in detail?
- Does the documentation provided record a description of the specific safety measures that are to be borne by the exporter?
- Has the documentation provided recorded a description of the specific security measures to be adopted by the importer?
- Has a copy of the contract between exporter and importer been provided?
- Does the contract match the relation between exporter and importer?
- In the case of the service being provided, has fulfilment of the contractual framework of provision of the service been accredited?
- Has accreditation of the powers of attorney of the signatories been provided?
- Has the degree of confidentiality of the documentation to be subject to public information been indicated?
- Has a declaration been provided of fulfilment of the duty to inform the company committee pursuant to 4.2 of the Workers' Statute
- Are all the participants in the transfers identified?
- May there be subcontracting that is not identified in the subcontract?

- Does the contract presented cover all the guarantees established in the Decision?
- Do the data categories included in international transfer coincide with the data categories recorded in the file inscription at the RGPD?
- Is disclosure of specially protected data foreseen?
- Has the responsibility clause been correctly included?

ANNEX. REGULATORY FRAMEWORK

1. Glossary

It is necessary to clarify the more specific terminology used in relation to international transfers:

- **International Data Transfer:** An international data transfer is considered to be data processing involving transmission of that data outside the territory of the European Economic Space, either as a cession or disclosure of data, or in order to perform data processing on behalf of the controller established in Spanish territory.

- **Personal data exporter:** the individual or corporation, power or private, or administrative body located in the Spanish territory who performs transferral of personal data to a third country under the terms provided in these Regulations.

- **Personal data importer:** the individual or corporation, power or private, or administrative body that receives the data in the event of international transferral to a third country, either the data controller, processor or a third party.

2. General framework

Article 1, paragraph two of Directive 95/46/EC by the European Parliament and Council, of 24 October 1995, on protection of individuals with regard to the processing of personal data and on the free movement of such data, establishes that "*Member States shall not restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1*".

Regulation of international transfers is considered in Articles 33 and 34 of Spanish Organic Act 15/1999, of 13 December, on Personal Data Protection.

In this regard, Article 33.1 indicates that "*neither temporary nor definitive personal data transfers may be performed when they have been processed or gathered for such processing in countries that do not provide an equivalent level of protection to that provided by this Act, except if, in addition to fulfilling the terms provided herein, prior authorisation is also secured from the Director of the Data Protection Agency, who may only grant it if the appropriate guarantees are obtained.*"

On the other hand, Article 33.2 establishes the criteria to determine the adequate nature of the protection to be provided: "*the adequate nature of the level of protection afforded by the destination country shall be evaluated by the Data Protection Agency according to all the circumstances arising in the transferral or category of data transferral. In particular, it must take into account the nature of the data and the purpose and duration of the processing foreseen, the country of origin and the final destination country, the general or sectorial rules of Law in force in the third country concerned, the content of the reports by the European Union Commission, as well as the professional rules and security measures in force in those countries".*

An exception to this authorisation shall only be made in the cases foreseen in Article 34 of the Act, or when the data is intended for a Member Country of the European Union, or countries covered by the Agreement on the European Economic Area, or regard to which the Commission of the European Communities has adopted a Decision of compliance with Directive 95/46/EC.

The cases foreseen in said Article 34 are as follows:

- When the international personal data transfer arises from application of treaties or conventions to which Spain is a party;
- When the transfer is performed in order to provide or request international judicial assistance;
- When the transfer is necessary for medical prevention or diagnosis, to provide health care or medical treatment, or management of health services;
- When it refers to monetary transfers according to their specific legislation;
- When the data subject has granted unequivocal consent to the transfer foreseen;
- When the transfer is necessary for performance of a contract between the data subject and the controller or to adopt pre-contractual measures taken at the request of the data subject;
- When the transfer is necessary to enter into or to perform a contract that has been arranged or is about to be formalised, in the interest of the data subject, by the controller and a third party;
- When the transfer is necessary or legally required to safeguard a public interest. This status shall be given to a transfer requested by a tax or customs authority in performance of its duties;
- When the transfer is necessary for recognition, exercise or defence of a right in judicial proceedings;

- When the transfer is performed at the request of a person with a legitimate interest, from a Public Registry and that is in keeping with its purpose.

On the other hand, an international data transfer does not exclude application of the provisions set forth in Organic Act 15/1999, according to its scope of application, and the Spanish Data Protection Agency is competent to verify its fulfilment.

With regard to notification of the transfers provided on the General Data Protection Register (RGPD), the LOPD establishes that any person or entity intending to perform an international data transfer must specifically record this when proceeding to notify the file to the RGPD.

2.1. To countries in the European Economic Area

Sending data to a country in the European Economic Area, even when it involves international movement of data for the purposes of application of the LOPD, is considered either a cession of data or provision of services and is thus subject to the terms provided in Articles 11, 12 and 21.

2.2 To countries with an adequate level of protection

In addition to the countries parties to the Agreement on the European Economic Area, that includes all the Member States of the European Union, as well as Liechtenstein, Iceland and Norway, the following are considered countries with an adequate level of protection for which the European Communities Commission has declared adequacy:

- Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland;
- Commission Decision 2000/520/EC of 26 July 2000, pursuant to Directive 95/46/EC of the European Parliament and of the Council, on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions, issued by the US Department of Commerce;
- Commission Decision of 20 December 2001, pursuant to Directive 95/46/EC of the European Parliament and of the Council, on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act;

- Commission Decision 2003/490/EC, of 30 June 2003, pursuant to Directive 95/46/EC of the European Parliament and of the Council, on the adequate protection of personal data in Argentina;
- Commission Decision 2003/821/EC, of 21 November 2003, on the adequate protection of personal data in Guernsey.
- Commission Decision 2004/411/EC, of 28 April 2004, on the adequate protection of personal data in the Isle of Man.

When it is foreseen to perform an international data transfer to one of these countries with the adequate level of protection, that transfer must be reported to the Agency by filling in the relevant section of the electronic form NOTA on file notification.

2.3 To countries that do not provide an adequate level of protection

International transferral of data to a country that does not provide a comparable level of data protection to that provided by the LOPD may only be performed if prior authorisation is secured from the Director of the Agency, under the terms set forth in section 3 of this document, or if that transfer is covered by any of the exceptions foreseen in Article 34 of the LOPD.

2.4 Exceptions to the authorisation

In the case of international data transfers covered by consent by the person concerned, one must take into account that, in order for that consent to be considered unequivocal, just as required under Article 34.e) of the LOPD, it shall be necessary for its application to record, in addition to the receiver of the transfer, the destination country, as well as the specific, set purpose for which the personal data is transferred.

In any case, when the transfer is authorised in any of the exceptions foreseen in said Article 34 of the LOPD, that transfer must be reported to the Agency by filling out the relevant section of the electronic form NOTA on file notification.

2.5 Authorisation of international data transfer

When the destination of an international data transfer is a country in which a comparable level of protection has not been recognised and the circumstances of Article 34 are not fulfilled, in addition to compliance with the terms of the LOPD, it is necessary to obtain

authorisation from the Director of the Spanish Data Protection Agency, pursuant to Article 33.1 of the LOPD.

This authorisation is only granted when the controller offers sufficient guarantees with regard to protection of private life, the fundamental rights and liberties of personal data protection, as well as with regard to exercise of those rights.

Those guarantees may arise, in particular from contractual clauses, foreseen under Article 25.2 of Directive 95/46/EC. In that sense, considering Article 26.4 de Directive, the Member States are bound by the Decisions of the Commission that establish contractual clauses to be applied to contracts between controllers and between controllers and processors. Three Decisions have now been published:

- Commission Decision 2001/497/EC, of 15 June 2001, on standard contractual clauses for the transfer of personal data transfers to third countries;
- Commission Decision 2002/16/EC, of 27 December 2001, on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC;
- Commission Decision 2004/915/EC, of 27 December 2004, amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries.

In this sense, one must bear in mind that the Member States shall be bound by any other future Decision that the Commission may adopt in fulfilment of the terms established in Article 26.4 of Directive 95/46/EC.
The Spanish Data Protection Agency, entrusted with of the legal powers to authorise international data transfers, has adopted the necessary measures to adjust to the aforesaid Commission Decisions.

2.6 Application for authorisation for international data transfers

The following details the procedure to apply for and arrange international data transfer authorisations, with an attached series of recommendations.

The procedure to obtain the authorisation for international data transfers to third countries referred to in Article 33 of Organic Act 15/1999, of 13 December on Data Protection shall usually be commenced at the request of the exporter intending to perform the transfer.

In any case, in the application to the Agency, the exporter must clearly and precisely state the purpose, the groups of parties concerned and the data subject with reference to the international transfer, as well as identification of the file or files affected by it, and the documentation including the required warranties to obtain the authorisation, providing a description of the specific security measures that are to be adopted, both by the data exporter as well as the importer.

When the information provided in the proceedings does not permit ascertaining the details stated above, the controller is required to provide all the necessary documentation and to clarify those points, in order to ensure the data to be transferred are adequate and appropriate for the purpose forming the object of the international transfer.

Submitting an application for an international transfer authorisation gives rise to the relevant proceedings at the General Data Protection Register. The General Data Protection Register may require the applicant, if the documentation is not complete or does not fulfil the formal requisites, or if the description of the transfer shows some inconsistency in processing the data, or in fulfilment of sufficient guarantees, in order that correction may be performed within the term of 10 days and the application be improved as required, pursuant and according to the terms of Article 71.1 of Act 30/1992.

If no answer is received within the term of 10 days, the case shall be declared closed by a relevant resolution of the Director. Notice of this shall be served on the applicant by the General Data Protection Register.

The procedural formalities continue with its investigation, in which the transfer and underlying matters are examined in detail in relation to the guarantees provided. If any clarification is required, the relevant correction requirement shall be issued. In any event, the Director of the Spanish Data Protection Agency shall hand down the Resolution to commence public information formalities to be published in the Official State Gazette. The term for correction is 10 days, suspending the procedure if no answer is received within that term.

The public information period is 20 days from publication in the Official State Gazette, a period during which those who see fit may have access to the relevant documentation on the international transfer subject to authorisation to make the allegations they consider appropriate, if necessary.

If allegations are received during this period, they shall be attached to the file, and the applicant notified, commencing the formalities to hear the party concerned within a term of 10 days.

Once that term has elapsed or, if appropriate, at the moment of receiving the allegations considered appropriate by the party concerned, and always before three months have elapsed from commencement of the proceedings, the Agency shall hand down the relevant justified resolution, putting an end to the procedure.

When the Director of the Spanish Data Protection Agency resolves to authorise the international data transfer, the authorisation resolution is reported to the General Data Protection Register, in order to proceed to its inscription, notifying the applicant and, once notified, it is published on the Agency web page.

Notification of this Resolution on authorisation or refusal of international data transfer is also given to the **Ministry of Justice**, in order to proceed to its notification to the **European Commission** and the other Member States of the European Union according to the terms set forth in Article 26.3 of Directive 95/46/EC.

2.7 Binding Corporate Rules

Authorisation may also be granted for international data transfer within multinational corporate groups when they have been adopted the same standards or internal rules that provide the necessary guarantees with regard to protection of private life and the fundamental right to data protection of the subjects and also guarantees fulfilment of the principles and exercise of the rights recognised under Organic Act 15/1999, of 13 December, and its implementation regulations.

The Binding Corporate Rules system has been developed in the following working documents of the European Data Protection Authorities Group (Article 29 Working Party):

- WP107, of 14 April 2005, setting forth a co-operation procedure for issuing common opinions on adequate safeguards resulting from “Binding Corporate Rules”;
- WP108, of 14 April 2005, establishing a model checklist application for approval of Binding Corporate Rules

- WP 74, of 3 June 2003, transfers of personal data to third countries: applying Article 26 (2) of Directive 95/46/EC, to the Binding Corporate Rules for International Data Transfers.

In this case, in order to proceed to authorisation by the Director of the Spanish Data Protection Agency, it shall be necessary for the standards or rules to be binding on the companies in the Group and enforceable under Spanish law.

In any case, the authorisation by the Director of the Spanish Data Protection Agency shall imply that the terms provided in the internal standards or rules are enforceable both by the Agency as well as by the subjects whose data has undergone processing.

.