

**EADS**

SIM DATA PROTECTION AND PRIVACY POLICY


PURPOSE

The SIM Privacy Policy is created to comply with legal and regulatory requirements, established in the European Data Protection Directive 95/46/EC and the national legislations. The compliance with legal and regulatory requirements is ensured by a set of functional and technical measures that shall be implemented within EADS.

The implementation of these measures shall ensure that personal data and specific business data related to the individual are gathered, stored and maintained in accordance with the European Data Protection Directive and national data Protection legislation of the countries in which EADS provides its goods and services.

SCOPE

This document applies to all EADS applications containing and managing personal data and specific business data related to the individual in France, Germany, Spain, United Kingdom and United States.



Owner's approval: (signed)

Date: 10.07.2008

Name: Cristiano Borrelli

Function: Head of SIM pgm. ops.



Authorization: (signed)

Date: 11.6.7.08

Name: Philippe LaFaudie

Function: Head of Program
SIM



SIM DATA PROTECTION AND PRIVACY POLICY

PURPOSE

The SIM Privacy Policy is created to comply with legal and regulatory requirements, established in the European Data Protection Directive 95/46/EC and the national legislations. The compliance with legal and regulatory requirements is ensured by a set of functional and technical measures that shall be implemented within EADS.

The implementation of these measures shall ensure that personal data and specific business data related to the individual are gathered, stored and maintained in accordance with the European Data Protection Directive and national data Protection legislation of the countries in which EADS provides its goods and services.

SCOPE

This document applies to all EADS applications containing and managing personal data and specific business data related to the individual in France, Germany, Spain, United Kingdom and United States.

Owner's approval: (signed)

Date:

Name:

Function:

Authorization: (signed)

Date:

Name:

Function:



Table of Contents

1. LEGAL FRAMEWORK	3
2. PERSONAL DATA CLASSIFICATION MODEL	4
2.1. Basic Level of Data	5
2.2. Medium Level of Data.....	5
2.3. High Level of Data.....	6
3. GENERAL REQUIREMENTS	6
4. LEGAL REQUIREMENTS AND STATUS PER COUNTRY	7
4.1. European Regulation	7
4.1.1. Directive 95/46/EC	7
4.1.1.1 Right of information in the collection of data	7
4.1.1.2 Consent of the data subject	7
4.1.1.3 Right of access, rectification or cancellation	7
4.1.1.4 Treatment on behalf of third parties	8
4.2 France	8
4.2.1. National legislation.....	8
4.2.1.1. Right of information in the collection of data	12
4.2.1.2. Consent of the data subject	12
4.2.1.3. Right of access, rectification or cancellation	13
4.2.1.4. Treatment on behalf of third parties	13
4.3 Germany	13
4.3.1. National legislation.....	13
4.3.1.1. Right of information in the collection of data	15
4.3.1.2. Consent of the data subject	16
4.3.1.3. Right of access, rectification or cancellation	16
4.3.1.4. Treatment on behalf of third parties.....	16
4.4 Spain	16
4.4.1. National legislation.....	16
4.4.1.1. Right of information in the collection of data.....	19
4.4.1.2. Consent of the data subject.....	20
4.4.1.3Right of access, rectification or cancellation	20
4.4.1.4. Treatment on behalf of third parties	20
4.5 United Kingdom	21
4.5.1. National legislation.....	21
4.5.1.1. Right of information in the collection of data.....	24
4.5.1.2. Consent of the data subject.....	24
4.5.1.3. Right of access, rectification or cancellation.....	24
4.5.1.4. Treatment on behalf of third parties	24
4.6 United States of America	25
4.6.1 National legislation.....	25
4.6.1.1.Right of information in the collection of data	25
4.6.1.2 Consent of the data subject.....	25
4.6.1.3 Right of access, rectification or cancellation	25
5. INTERNATIONAL TRANSFER OF DATA	26



1. LEGAL FRAMEWORK

The legal framework for data protection within the European Union is comprised by European Directives, which have been transposed into several national laws that apply in each Member State. The different national laws establish the binding points of the European Directive. For the purposes of this document, only the European Directive and the national laws related to data protection are covered for the European countries considered as EADS core countries.

Outside of the European Union, the present document will only consider the legal framework of the United States.

EUROPEAN UNION

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

EADS CORE COUNTRIES

FRANCE

- Law n° 78-17 of 6th of January 1978 concerning Information Systems, Files and Freedom.
- Law n° 2004-801 of August 2004 concerning Protection of Personal Data.

GERMANY

- Federal law 21st January 1977 modified by Federal law of 20th December 1990
- Federal law 20th December 1990 modified by Federal law 14th September 1994 and by the Federal Data Protection Act of 18th May 2001.

SPAIN

- Ley Orgánica 15/1999 of December 13th on the Protection of Personal Data.
- Real Decreto 994/1999, of June 11th, which approves the Regulation on Mandatory Security Measures for the Computer Files which contain Personal Data.

UNITED KINGDOM

- Data Protection Act 16th of July 1998.

UNITED STATES OF AMERICA

- Federal System of legal data protection in place.
- The "Safe Harbor Agreement" of November 1st, 2000.



2. PERSONAL DATA CLASSIFICATION MODEL

Data Protection legislation pursues the protection of fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the **European Convention for the Protection of Human Rights and Fundamental Freedoms** and in the general principles of Community law.

The **European Directive** establishes the classification of *special categories of data*, which are capable by their nature of infringing fundamental freedoms or privacy. These special categories of data are, the following: "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" (Article 8 of the European Data Protection Directive). These data should not be processed unless the data subject gives his/her explicit consent.

The **UK Data Protection Act** defines personal data and sensitive personal data.

The definition of personal data is "data which relates to a living individual who can be identified

(a) from those data, or

(b) from data and other information which is in the possession of, or is likely to come into the possession of the data controller." (Data Protection Act 1998 – Part I.1 (1))

"Sensitive personal data means personal data consisting of information as to: the racial or ethnic origin of the data subject; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; physical or mental health or condition; sexual life; perpetration or alleged perpetration of an offence; any proceedings for any offence committed or alleged to have been omitted by him/her, the disposal of such proceedings or the sentence of any court in such proceedings" (Data Protection Act 1998 – Part I.2).

***Germany** and **France** do not establish different categories of data, so the classification made in the Directive is binding in these countries.

*The **Spanish** Personal Data Classification Model is based on article 4 of the Royal Decree 994/1999 of 11 June, which approves the Regulation on mandatory Security Measures for the computer files, which contain personal data.

Taking into account the European Directive and the national legislation in UK, Germany, Spain and France and extrapolating these to the other countries in scope of this policy, the **EADS personal data classification model** establishes three levels of data sensitivity:

Basic

Medium

High

Data classification levels and sample fields are explained below:



2.1. Basic Level of Data

Data Classification level BASIC

Personal Details	Data which identify the data subject(s) and their personal characteristics: Name, address, contact details, age, gender, date of birth, physical description, passport, picture, voice, digital signature, etc.
Family, lifestyle and social circumstances	Matters relating to the family of the data subject and the data subject's lifestyle and social circumstances: current marriage and partnerships and marital history details, leisure activities, membership of charitable or voluntary organizations, military service...
Education and training details	Matters which relate to the education and professional training of the data subject: academic records, qualifications, skills, training records, professional expertise, student and pupil records.
Employment details	Matters relating to the employment of the data subject: employment and career history, recruitment and termination details, attendance record, performance appraisals, training records, security records...
Goods or services provided	Classes of data relating to goods and services, which have been provided. Examples are details of the goods or services supplied, licenses issued, agreements and contracts.

2.2. Medium Level of Data

Data Classification level MEDIUM

Financial details	Matters relating to the financial affairs of the data subject: income, salary, asset and investments, payments, creditworthiness, loans, benefits, grants, insurance details, pension information.
-------------------	--



2.3. High Level of Data

(Data Classification level HIGH (SENSITIVE))

<i>Treatment of sensitive data usually includes trade union membership data in the enterprise and/or employee health data necessary for fiscal purposes.</i>	
Racial or ethnic origin	Political opinions
Religious or philosophical beliefs	Trade union membership
Physical or mental health condition	Health or sexual orientation
Offences (*)	Proceedings relating to offences (*)

(*) when authorized by local legislation

3. GENERAL REQUIREMENTS

The European Data Protection Directive establishes different binding measures to guarantee the security of personal data.

These measures are classified into:

- Technical measures
- Functional measures
- Legal requirements

The European Directive does not include any definitive measures to be carried out, although the law in some member states (national laws) establishes **technical** and **functional measures** to be applied. Note that **legal requirements** are established both in the European Directive and in the national laws.

(a) Examples of **technical measures** to be applied:

- Access control (logical)
- Temporary files
- Identification and authentication
- Record of incidents
- Management of media
- Back up copies and recovery
- Test with real data
- Security Document

(b) Examples of **functional measures**:

- Functions and obligations of staff
- Security officer
- Working outside the premises where the file is located
- Record of incidents
- Access control (physical)



- Access record
- Management and distribution of media
- Audit

(c) The **legal requirements** established in the European Directive are:

- Right of information in the collection of data (article 10).
- Consent of the data subject for high-level data (article 8).
- Duty of secrecy (article 16).
- Access of data on behalf of third parties (article 19).
- Right of access, rectification or cancellation (article 12).

4. LEGAL REQUIREMENTS

The legal requirements established in the European Directive and in the national laws are explained in this chapter. In the cases where the national law does not include any specific measures, the principles established in the Directive are binding.

All EADS group entities will take the necessary steps to comply with the legal requirements below.

4.1 EUROPEAN REGULATION

The Directive 95/46/EC imposes four steps:

4.1.1.1 Right of information in the collection of data

The Directive establishes the legal framework for the information that has to be provided to the person from whom data relating to him/herself is collected.

4.1.1.2 Consent of the data subject

Article 7 of the European Directive establishes that Member States shall provide that personal data may be processed only if the data subject has unambiguously given consent.

4.1.1.3 Right of access, rectification or cancellation

Article 12 of the European Directive establishes that Member States shall guarantee every data subject the right to obtain from the controller:

- Confirmation as to whether or not data relating to him/her is being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data is disclosed,
- Communication to him/her in an intelligible form of the data undergoing processing and of any available information as to their source,
- The rectification, erasure or blocking of data when the processing does not comply with the provisions of this Directive, in particular due to incomplete or inaccurate nature of the data.



The communication must follow the procedure established in each national law, taking into consideration the exceptions that apply in each country.

4.1.1.4 Treatment on behalf of third parties

Article 17 of the European Directive establishes that organizational and technical measures have to be set up in order to assure the security of personal data. In case of third parties, where processing is carried out on its behalf, the controller has to choose a processor providing sufficient guarantees that the right measures governing the processing will be carried out, and must ensure compliance with those measures.

The compliance with its responsibilities of the processor must be governed by a contract or legal act binding the processor to the controller and stipulating the measures that the processor must apply for the treatment of personal data.

4.2 FRANCE

4.2.1 National Legislation

Status of implementation of the Directive

The Data Protection Directive 95/46/EC have been implemented by the Law of august 2004 concerning the protection of personnel data (the "DPA").

Entry into force of the implementing legislation

The DPA entered into force on 6th of august 2004.

Territorial scope of application

The DPA applies to processing of personal data where:

- (i) the data controller is established in France (the controller is considered as established when its activities are carried out in the context of an establishment regardless of its legal status); and
- (ii) the data controller is not established in France or in Community territory and, for purposes of processing personal data, makes use of equipment located in France, unless such equipment is used only for purposes of transit through France or another Member State.

The data controller is defined in Chapter 1 article 3 as "a person, public authority, department or any other organization who determines the purposes and means of the data processing"

Material scope of application

The DPA applies to both automatic processing and manual processing.

Personal scope of application



The DPA only applies to data relating to individuals and not to legal entities.

Entity responsible for compliance with the National Legislation

The data controller is responsible for compliance with the DPA. The data controller is defined as the natural or legal person, public authority, agency or any other body that determines the purposes and means of the processing.

National Regulatory Authority competent with regard to personal data protection

Commission Nationale de l'Informatique et des Libertés or "CNIL"
8 rue Vivienne, CS 30223
75083 paris, cedex 02

www.cnil.fr

Notification or registration scheme and timing

Any processing of data shall be notified. The data controller has to **fill in a declaration form** available on the CNIL website. Simplified forms requiring minimum information to be provided are available for the most typical processing (e.g. payroll, management of employees, customer files). **The notification must take place prior to collecting and processing the data, which can only start from the date the data controller receives a receipt from the CNIL.**

Exemptions

All processing of personal data must be notified except:

- (i) processing whose sole purpose is the keeping of a register which, according to laws or regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest;
- (ii) processing for which the data controller has appointed a personal data protection officer responsible for insuring the application of the obligations provided by the law, for keeping a register of processing, except where a transfer to a non-Member State is contemplated.

Rules on the quality of the data processed

The data shall be

- (i) fairly and lawfully collected and processed, and
- (ii) collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

The data shall be

- (i) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed, and



- (ii) accurate, complete and, where necessary, kept up to date.

Appropriate steps must be taken to ensure that data that are inaccurate or incomplete in relation to the purposes for which they were collected or further processed, are erased or rectified.

Retention period

The data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or further processed.

Right to information

The data subject shall be provided by the controller or his/her representative with the following information:

- (i) the identity of the controller and of his/her representative, if any;
- (ii) the purposes of the processing;
- (iii) whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply;
- (iv) the identity of the recipients or the category of recipients to which the recipients belong;
- (v) the existence of the right of access to and the right to rectify his/her personal data; and
- (vi) in the case of international transfer of data to a non-EU Member State, information on such transfer.

Right of access/correction/objection & other rights

Access: Data subjects have the right to obtain from the controller:

- (i) confirmation as to whether or not its data are being processed;
- (ii) information regarding the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;
- (iii) in the case of international transfer of data outside to a non-EU Member State, information of such transfer;
- (iv) communication in an intelligible form of the data and of any available information as to their source; and
- (v) the logic involved in the processing. **A copy of the data processed is provided to the data subjects.** The controller may object to abusive queries from the data subjects.

Rectification: Data subjects also have the **right to ask the controller to rectify, complete, update, block or erase their data when they are incomplete, inaccurate** or when the use, the transfer or the storage of such data is forbidden.

Object to processing: Data subjects have the right to object at any time to the processing of their personal data on compelling legitimate grounds. Data subjects also have the right to object, free of charge, to the processing of their personal data for direct marketing purposes by the current or future data controller.



Security requirements in order to protect the data

The data controller or any person acting under its instructions must implement appropriate technical and organizational measures to safeguard the security of the personal data, in particular, in order to avoid any distortion, damage or unauthorized disclosure to a third party. The measures implemented shall ensure a level of security appropriate to the risks arising out of the process and the nature of the personal data.

Specific rules governing processing by a third party (processor) on behalf of data controller

Wherever a sub-contractor is involved (a processor acting on behalf of the data controller being viewed as a sub-contractor) the data controller shall ensure that:

- (i) the sub-contractor presents sufficient guarantees to enable the implementation of the security and confidentiality measures and that the sub-contractor complies with the same security requirements; and
- (ii) the contract with the subcontractor contains all necessary provisions in terms of security of the treatment. In addition, the subcontractor only acts upon instruction of the provider and the data controller remains in all cases jointly liable with respect to the security and confidentiality of the personal data.

Transfer within the EEA

The transfer of data to countries ensuring an adequate level of protection **only requires that the data controller:**

- (i) informs the data subject; and**
- (ii) fills out a declaration with the CNIL, which delivers a receipt enabling the transfer without delay.**

Transfer outside the EEA

When a transfer to a country that does not ensure an adequate level of protection is contemplated, the data controller can annex to its declaration to the CNIL the Standard Contractual Clauses issued by the European Commission. According to the CNIL, the consent of the individual is not sufficient when a transfer to a country not ensuring an adequate level is massive, repetitive or structural. The CNIL considers that transfers have such nature in most of the cases. Therefore, the derogations provided in the Directive and the DPA would only apply to isolated or quantitatively limited transfers or in very limited cases of urgency (e.g. in order to protect the vital interests of the data subject). The data subject's consent is never deemed sufficient when the transfer relates to employees' personal data.

The processing of data revealing directly or indirectly racial or ethnic origin, political opinions, religious or philosophical beliefs, sex life, health data or judicial data is restricted under French law. These data may only be processed under specific circumstances described in the draft DPA.



For an updated list of countries that do not ensure an adequate level of protection, please refer to www.cnil.fr

Enforcement - Sanctions

The Law provides for criminal sanctions in addition to civil sanctions already available. It does not, however, provide for any regulatory fines. The draft DPA will introduce under French law the option for the CNIL to fine data controllers in the event of breach of the draft DPA.

4.2.1.1 Right of information in the collection of data

Article 32 Law n° 78-17 modified by law of 6th august 2004, concerning the protection of personnel data, establishes that the controller must provide information prior to the data treatment on:

1. The mandatory or facultative character of the data collection
2. The identity of the data controller.
3. Purpose of the data collection.
4. Consequences in the event that the employee does not answer.
5. A description of any recipient(s) to whom the data controller intends or may wish to disclose the data.
6. The access and rectification rights.
7. The opposition right.
8. Data transfer to an EU member State or not.

4.2.1.2 Consent of the data subject

The data subject shall give the company his or her unambiguous consent for the collecting of sensitive data as defined in article 8 Law 78-17 modified by law of 6th august 2004 concerning the protection of personnel data.

Data subject has the right, for rightful reasons; to disagree that personal data should be processed (article 38 Law 78-17 modified by law of 6th august 2004 concerning the protection of personnel data).

4.2.1.3 Right of access, rectification or cancellation (Articles 39 to 43 Law n° 78-17 modified by law of 6th august 2004 concerning the protection of personnel data)

- Access right (article 39)

The data subject shall, at his request, be provided with information on:

1. Stored data concerning him/her, including any reference in them to their origin.
2. The recipients or categories of recipients to whom the data is transmitted.
3. The purpose of storage

- Right of rectification and cancellation

Incorrect personal data shall be corrected. If it is established that personal data is incorrect, or if the data subject contests their correctness, this situation has to be recorded in an appropriate manner by the company.



4.2.1.4 Treatment on behalf of third parties

According to French legislation, no additional measures need to be applied for the treatment of data by third parties apart from the measures and limits established by the European Directive.

4.3 GERMANY

4.3.1 National Legislation

Scope of implementation of the Directive

The Data Protection Directive 95/46/EC has been implemented into German law under the German Federal Data Protection Act (Bundesdatenschutzgesetz - the "**DPA**").

Entry into force of the implementing legislation

The DPA came into force on 23 May 2001.

Territorial scope of application

The DPA is only applicable to data controllers located in Germany and does not apply to data controllers located in another Member State of the EU or the EEA, except where collection, processing or use of personal data is carried out by a branch in Germany (principle of origin). The DPA is also applicable to data controllers not located in a Member State of the EU or the EEA who collect process or use personal data in Germany (principle of territoriality).

Material scope of application

The DPA is only applicable to the collection, processing and use of personal data by means of data processing systems and non-automated filing systems, such as manual record cards.

Personal scope of application

The DPA only applies to information concerning personal or material circumstances of an identified or identifiable individual and does not apply to legal entities.

Entity responsible for compliance with the National Legislation

The responsibility for complying with the provisions set out in the DPA is borne by the data controller. The data controller is defined as any person or body that collects processes or uses personal data on its own behalf or commissions others to undertake the same on its behalf.

Notification or registration scheme and timing

There are 20 different regional supervisory authorities responsible for monitoring the implementation of data protection. The names, addresses and websites of these supervisory



authorities are available at www.bundesdatenschutz.de (select "Anschriften und Links" and then " Die Aufsichtsbehörden für den nicht-öffentlichen Bereich").

Notification or registration scheme and timing

Automated processing procedures are required to be registered with the competent supervisory authority in advance. This does not apply, if :

- the data controller has appointed a data protection official (which is usually the case in Germany), or
- the controller collects, processes or uses personal data for its own purposes, provided that a maximum of nine employees are concerned with it and either consent has been obtained from the data subject or it serves the purpose of a contract or a quasi-contractual fiduciary relationship with the data subject.

Those exceptions do not apply if the data controller commercially stores personal data for the purpose of transfer or anonymised transfer.

Rules on the quality of the data processed

Personal data must be accurate and kept up-to-date at all times. The data controller is only allowed to handle personal data which are absolutely necessary for legitimate purposes.

Retention period

Personal data can only be kept as long as necessary for the purpose of processing.

Right to information

The data controller is obliged to inform the data subject if personal data are collected from the data subject or if personal data are stored for the first time for the data controller's own purposes without the data subject's knowledge. The data subject must be notified, inter-alia, regarding the type of data collected or stored, the purpose of their collection, and the identity of the data controller, unless the data subject has been informed of this via another source.

Right of access/correction/objection & other rights

The **data subject may request to see such information at any time. The data subject may demand the correction of incorrect data as well as the deletion or blocking of personal data, the storage of which is not, or is no longer, covered by legitimate purposes.** The data subject has the right to object to personal data being transferred for purposes of advertising, market and opinion research.

Security requirements in order to protect the data

Public and private bodies processing personal data, either on their own behalf or on behalf of others (Processors) are obliged to ensure that all technical and organizational measures necessary are taken in order to comply with the provisions set out in the DPA. Pursuant to the Annex to the



DPA, measures must be taken with regard to access control, transmission control, input control and availability control.

Specific rules governing processing by a third party (processor) on behalf of data controller

In the event that a third party (processor) is handling personal data on behalf of a data controller, the processor and the data controller need to conclude a written agreement on the commissioned processing of data and specify, inter-alia, the details of the handling of the personal data. Where processors are commissioned to handle data, the responsibility for compliance with the provisions of the DPA is borne by the data controller. Therefore, the controller must ensure that the data are processed strictly in accordance with its instructions (job control).

Transfer within the EEA

If the general provisions for the transfer of personal data set out in the DPA have been complied with, the transfer of personal data to Member States of the EU or the EEA and to countries that guarantee an adequate level of data protection is permissible without any other additional requirements.

Transfer outside the EEA

If the general provisions for the transfer of personal data set out in the DPA have been complied with, transfer of personal data to the U.S. is permissible if the data importer has signed up to the Safe Harbor and transfer to all other countries is permissible if

the EC Model Clauses are complied with, or
the data subject has given his/her consent, or
the transfer is necessary for the fulfillment of a contract with the data subject, or
Corporate Binding Rules have been effectively implemented.

The transfer has to be registered with the competent supervisory authority.

Enforcement - Sanctions

Should a data controller infringe the data subject's rights under the DPA, the data subject is entitled to injunctive relief and compensation for damages. In addition, the competent governmental authority can impose administrative fines and penalties in case of a violation of the DPA.

4.3.1.1 Right of information in the collection of data (Section 34 of the German Federal Data Protection Act)

Data subject shall, upon request, be provided with information on:

1. Stored data concerning him/her, including any reference in them to their origin.
2. The recipients or categories of recipients to whom the data is transmitted.
3. The purpose of storage.



The request should specify the type of personal data on which information is to be provided.

4.3.1.2 Consent of the data subject

Consent shall be effective only when based on the data subject's free decision. He or she shall be informed of the purpose of collection, processing or use and, in so far as the circumstances of the individual case dictate or at his or her request, of the consequences of withholding consent. Consent shall be given in writing unless special circumstances warrant any other form. If consent is to be given together with other written declarations, it shall be made distinguishable in its appearance (section 4 German Federal Data Protection Act).

4.3.1.3 Right of correction, erasure or blocking of data (Section 35 German Federal Data Protection Act)

Right of rectification and cancellation

Incorrect personal data shall be corrected. If it is established that personal data is incorrect, or if the data subject contests their correctness, this situation has to be recorded in an appropriate manner by the company.

4.3.1.4 Treatment on behalf of third parties (Section 11 German Federal Data Protection Act)

German law permits the transfer of data to fulfill the purposes of a contractual relationship. In that sense, German law considers that the subsidiaries of a company are third parties, even if the parent company owns the subsidiary 100%. The Act establishes that the third party to whom the data has been transferred can process or use the transferred data only for the purpose for which they were transferred to him/her.

The German Act does not include the obligation to sign a contract between the parties, but establishes the obligation for both, the controller and the processor, to apply the security measures established by the Law.

4.4 SPAIN

4.4.1 National Legislation

Status of implementation of the Directive

Directive 95/46/EC has been implemented by the Organic Law 15/1999, relating to Personal Data Protection (Ley Orgánica 15/1999, de Protección de Datos de Carácter Persona) (the "DPA").

Entry into force of the implementing legislation

The DPA entered into force on 14th January 2000.

Territorial scope of application



The DPA is applicable to processing carried out by a data controller established in Spain and by a data controller not established in the European Union but using equipment situated in Spain for purposes other than the mere transit of data. The DPA is also applicable to processing carried out by a data processor established in Spain (for example, the data processor will have to comply with the Security Measures Regulations).

Material scope of application

The DPA applies to both manual and electronic files. The processing of data already held in manual filing systems on the date of entry of the DPA shall be brought into conformity by 24 October 2007.

Personal scope of application

The DPA only applies to individuals. Legal entities do not fall within the scope of application of the DPA.

Entity responsible for compliance with the National Legislation

Controllers and processors are responsible for compliance and shall be subject to the sanctioning provisions of the DPA. The controller is defined as the public or private natural or legal person, or agency of the administration, which determines the purpose, content and use of the data processing. The processor is defined as the natural or legal person, public authority, agency or any other body that alone or jointly with others processes personal data on behalf of the controller.

National Regulatory Authority competent with regard to personal data protection

Agencia Española de Protección de Datos ("**AEPD**")
Sagasta, 22
28004 Madrid (Spain)
www.agpd.es

Notification or registration scheme and timing

Any person intending to create personal data files is required to register with the AEPD by completing the forms (available on the AEPD website). The General Data Protection Register of the AEPD approves the notification if the notification form complies with the necessary requirements. It is a mere filing of information that must take place prior to the creation of the data file (no further deadline). Any changes in the processing must be notified within the month of the change.

Exemptions

There are no exemptions from notification/registration.

Rules on the quality of the data processed

The data processed must be



adequate, relevant and not excessive in relation to the purposes of the processing and accurate and, where necessary, kept up-to-date.

Retention period

Personal data shall be kept for the periods stipulated in the applicable provisions or in the contractual relations, if any, between the controller and the data subject. Personal data shall be erased when they have ceased to be necessary or relevant for the purpose for which they were collected or recorded. They shall not be kept in a form permitting identification of the data subject for longer than necessary for the purposes for which they were collected or recorded.

Right to information

Data subjects from who personal data are requested shall previously **be informed expressly, precisely and unambiguously of:**

the existence of a personal data filing or processing system, the purpose of the collection of such data and the recipients of such information;
the obligatory or voluntary nature of their reply to the questions put to them;
the consequences of the collection of the data or of the refusal to supply them;
the possibility of exercising the rights of access, rectification, erasure and opposition; and
the identity and address of the controller or its representative, if any.

Furthermore, where questionnaires or other printed forms are used for the collection of personal data, they shall set out, in clearly legible form, the information referred to above.

Right of access/correction/objection & other rights

Data subjects **have the right to access their data and to rectify them when necessary.** They also have the right to object to the processing under specific circumstances.

Data subjects have the right:

Not to be subject to a decision that produces legal effects based solely on automated procession of data;
to consult the General Data Protection Register; and
to compensation if they have suffered damage or injury to their property or rights as a result of the infringement of the DPA.

Security requirements in order to protect the data

Royal Decree 994/1999, of 11 June, approved the "Security Measures Regulations", which classify the measures imposed on three levels: basic, medium and high, depending on the nature of the information processed.

Specific rules governing processing by a third party (processor) on behalf of data controller



The performance of processing operations by a processor on behalf of a controller **must be governed by a contract** that must be in writing or another form permitting its conclusion and contents to be evidenced.

The processing contract shall expressly stipulate that the processor shall only process the data in accordance with the instructions of the controller, that it shall not process the data for purposes other than those provided in such contract nor disclose the data, even for storage purposes, to other persons.

Once the contractual obligations have been performed, the personal data must be destroyed or returned to the controller, together with any medium or document in which any personal data that is the subject of processing are recorded.

Transfer within the EEA

The DPA authorizes the transfer of data within the EEA.

Transfer outside the EEA

The principle is that international transfers to countries that do not provide an equivalent level of protection as provided under Spanish law is prohibited, unless prior authorization has been granted by the Director of the Data Protection Agency. The DPA set out a number of derogations where Prior authorization shall not be required. Whether or not the transfer requires prior authorization, it has to be notified to the AEPD. In this regard, the standard form to notify the creation of data files includes a section on international transfers. If this section was not completed when the file was initially notified, the notification must be amended to include the transfer.

Personal data revealing ideology, trade-union membership, religion and beliefs may only be processed with the express, written consent of the data subject. Personal data relating to racial origin, health or sex life may only be obtained, processed and disclosed when so provided by a law on grounds of general interest, or with the data subject's express consent. Data files containing sensitive data must implement high-level security measures (in addition to basic and medium security measures they must, among other duties, encrypt the information when distributing it, etc.) as set out in the "Security Measures Regulations")

Enforcement - Sanctions

Spain has one of the most stringent penalty systems in the entire European Union in the event of breach of the DPA, with fines of up to EUR 601,012.10. The penalties established pursuant thereto range from EUR 601.01 to EUR 601,012.10, depending on the severity of the breach. Breach of the DPA implies fines but it must be noted that the Spanish Criminal Code also establishes a number of criminal offences derived from the violation of secrets and breach of privacy.

4.4.1.1 Right of information in the collection of data

Article 5 of the Organic Law on the Protection of Personal Data, establishes that data subjects from whom personal data is requested must **previously be informed explicitly, precisely and unequivocally of the following:**

1. The existence of a file or personal data processing operation, the purpose of collecting the data, and the recipients of the information.



2. The obligatory or voluntary nature of the reply to the questions put to them.
3. The consequences of obtaining the data or of refusing to provide them.
4. The possibility of exercising rights of access, rectification, erasure and objection.
5. The identity and address of the controller or of their representative, where applicable.

4.4.1.2 Consent of the data subject

Spanish Organic Law 15/1999 of 13 December on the Protection of Personal Data establishes in Article 6 the following:

1. Processing of personal data shall require the unambiguous consent of the data subject, unless otherwise established by law.
2. Consent shall not be required where the personal data is collected for the exercise of the functions proper to public administrations within the scope of their responsibilities; where they relate to the parties to a contract or preliminary contract for a business, employment or administrative relationship, and are necessary for its maintenance or fulfillment; where the purpose of processing the data is to protect a vital interest of the data subject under the terms of Article 7(6) of this Law or where the data is contained in sources accessible to the public and their processing is necessary to satisfy the legitimate interest pursued by the controller or that of the third party to whom the data is communicated, unless the fundamental rights and freedoms of the data subject are jeopardized.

4.4.1.3 Right of access, rectification or cancellation (Articles 15 to 17 Organic Law on the Protection of Personal Data)

- Right of access

The data subject shall have the right to request and obtain free of charge information on his or her personal data subjected to processing, on the origin of such data and on their communication or intended communication. The Controller must implement the right of access within a period of one month.

- Right of rectification and cancellation

The controller shall be obliged to implement the right of rectification or cancellation of the data subject within a period of ten days.

4.4.1.4 Treatment on behalf of third parties (Article 12 Organic Law on the Protection of Personal Data)

Spanish law provides that every data treatment on behalf of third parties must be governed by a contract or legal act binding the processor to the controller including the security measures that have to be set up assuring the quality of data. This contract will expressly lie down:

- The processor will process the data only in accordance with the instructions of the controller,
- Will not apply or use them for a purpose other than that set out in the said contract,
- Will not communicate them to other persons even for their preservation,
- Shall also set out the security measures, which the processor is obliged to implement,
- Once the contractual service has been provided (ended), personal data must be destroyed or returned to the controller, including any media or documents containing personal data.



4.5 UNITED KINGDOM

4.5.1 National Legislation

Status of implementation of the Directive

Directive 95/46/EC has been implemented by the Data Protection Act 1998 (the "DPA") dated 16th July 1998.

Entry into force of the implementing legislation

The majority of the provisions came into force on 1st March 2000.

Territorial scope of application

The DPA applies to data controllers in respect of any data if:

the data controller is established in the UK (including offices, branches, agencies or other regular practice in the UK) and data are processed in the context of that establishment; or
the data controller is established outside the EEA, but uses equipment in the UK for processing personal data other than for transit purposes.

Material scope of application

The DPA applies to both manual and electronic files. The manual files must form part of an organized filing system.

Personal scope of application

The DPA only applies to data relating to individuals.
In order for the DPA to apply, such individuals must be identifiable from:

the data; or
the data and other information which is, or is likely to come into, the possession of the data controller.

Entity responsible for compliance with the National Legislation

The data controller is responsible for compliance with the DPA. The DPA defines a data controller as a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

National Regulatory Authority competent with regard to personal data protection

The Information Commissioner
Wycliffe House



Water Lane
Wilmslow
Cheshire SK9 5AF

www.informationcommissioner.gov.uk

Notification or registration scheme and timing

Unless the processing is exempt, personal data may not be processed by a data controller that has not submitted notification to the Information Commissioner. No approval is required. The notification must occur prior to the first processing of personal data.

Exemptions

Every data controller who is processing personal data **must notify the Information Commissioner** unless they are exempt.

Exemptions apply in respect of:

- staff administration;
- advertising and marketing etc. of the data controller's business;
- accounts and records of the data controller or its customer/supplier; and
- certain processing relating to non-profit making organizations.

Rules on the quality of the data processed

The rules are set out in the data protection principles listed in the DPA. The third data protection principle states that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. The fourth principle states that personal data shall be accurate and, where necessary, kept up-to-date.

Retention period

The fifth data protection principle states that personal data processed for any purpose shall not be kept longer than is necessary for that purpose.

Right to information

Upon written request, any data controller must inform the individual whether it has processed or is processing any data concerning him/her. If it does, it must describe the personal data, the purpose for which they are processed and third parties to which they are, or may be, disclosed. Where data are processed automatically and are likely to form the sole basis for a decision significantly affecting the data subject, he/she will be entitled to know the logic involved in that decision making, provided it is not confidential.

Right of access/correction/objection & other rights

Access: Data subjects may obtain copies of their personal data **on written request** to data controllers.



Rectification: In certain cases, the data subject may ask the court to order the data controller to rectify, block, erase or destroy the data.

Objection to processing: An individual may in writing require that the data controller cease processing either generally or for a specified purpose or in a specified manner data concerning the individual if such processing is likely to cause substantial damage or distress to the individual or a third party and that damage/distress would be unwarranted.

Other: A data subject may require in writing that a data controller stop processing data for direct marketing purposes. In certain cases a data subject may object to decisions being taken about him/her based solely on automatic processing.

Security requirements in order to protect the data

Appropriate technical and organizational measures must be taken against unauthorized or unlawful processing and against accidental loss or destruction of, or damage to, personal data. Data controllers must ensure an appropriate level of security for the processed data having regard to possible damage and the nature of the data. The adequacy of measures taken is to be judged with regard to the state of technology and the cost of such measures.

Specific rules governing processing by a third party (processor) on behalf of data controller

The processing of personal data by a data processor must be in accordance with a written contract with the data controller requiring the processor to act only on instruction from the data controller and requiring the data processor to comply with the obligations equivalent to those imposed on the data controller by the seventh principle (security).

Transfer within the EEA

The DPA permits transfers within the EEA.

Transfer outside the EEA

The DPA prohibits transfers outside the EEA unless the destination ensures adequate protection for that data. Adequacy is to be assessed by the data controller. Personal data can be transferred outside the EEA under the usual circumstances (e.g. if there has been a Community adequacy finding, the data importer has signed up to the Safe Harbor or the EC Model Clauses, the data subject has consented or the transfer is necessary for the performance of a contract). A number of more minor grounds also exist.

Special protection is provided for personal data that are sensitive, i.e. concerning the data subject's racial or ethnic origin, political opinions, religious or similar beliefs, membership of a trade union, physical or mental health or conditions, sexual life, commission of an offence or proceedings for an offence.

Enforcement - Sanctions

Breaches may incur civil liability or criminal sanctions, which include unlimited fines (including for directors) but not jail terms. A breach of a data protection principle is not of itself a criminal offence, but may result in an Enforcement Notice. Breach of that notice may be a criminal offence.



4.5.1.1 Right of information in the collection of data

Article 7 of the 1998 Data Protection Act relates to Rights of Data Subjects and Others and states that the individual has the right to:

1. Know the name of the controller holding the information.
2. Know if the controller has a representative who is also holding information.
3. A description of the data being processed.
4. A description of who the data may be shared with.
5. The purpose of the processing.
6. Whether the processing is automatic.
7. Whether the information is being transferred to areas outside the EEA.

4.5.1.2 Consent of the data subject

Processing of personal data shall be in line with the conditions of Schedule 2 of the Act:

1. Consent of individual
2. Necessary in relation to a contract
3. Compliance with legal obligation of the data controller
4. To protect the vital interest of the individual
5. Necessary for administration of justice
6. Legitimate interests of the data controller

And in the case of sensitive personal data with the conditions of Schedule 2 plus Schedule 3.

4.5.1.3 Right of access, rectification or cancellation (Section 7 Data Protection Act 1998)

The controller must inform the data subject about any data that are being processed:

- The personal data of which that individual is the data subject,
- The purposes for which they are being or are to be processed, and
- The recipients or classes of recipients to whom they are or may be disclosed,

The controller has to communicate to him/her in an intelligible form all of the following:

- The information constituting any personal data of which that individual is the data subject
- Any information available to the data controller as to the source of that data
- Where the automatic processing of personal data of which that individual is the data subject, for the purpose of evaluating matters relating to him/her such as, for example, performance at work, creditworthiness, reliability or conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him/her, the communication by the data controller of the logic involved in the taking of that decision.

4.5.1.4 Treatment on behalf of third parties (Seventh Principle Data Protection Act 1998)

UK legislation introduces express obligations upon data controllers when the processing of personal data is carried out by a data processor on behalf of the data controller.



The obligations are the following:

- Choose a data processor providing sufficient guarantees in terms of the technical and organizational security measures it takes.
- Take reasonable steps to ensure compliance with those measures, and
- Ensure that the processing by the data processor is carried out under a contract, which is made in writing, under which the data processor should act only on instructions from the data controller. The contract must require the data processor to comply with obligations imposed to the data controller.

4.6. UNITED STATES OF AMERICA

4.6.1 National Legislation

The "**Safe Harbor Agreement**" extends, to some extent, the EU directive requirements to the USA. American organizations can certify themselves as following certain privacy protection principles, and can then import personal information from people and organizations in EU.

4.6.1.1 Right of information in the collection of data

A broad range of personnel information can be provided to the parent corporation and thus to EADS Group HR/PP as it centralizes the role over the Group's Human Resources functions. Several federal, state and local statutes and regulations contain restrictions on the disclosure of employee medical records. As EADS Group HR/PP has esteemed this to be High Sensitive Data and does not request High Sensitive Data, no restrictions apply here.

4.6.1.2 Consent of the data subject

With regard to non-medical personnel records, there are no substantial restrictions on disclosure of such information from a U.S. subsidiary to its foreign parent.

4.6.1.3 Right of access, rectification or cancellation

An employees' right to access, rectify or object to his personal data being processed in a legal manner not foreseen.



5. INTERNATIONAL TRANSFER OF DATA FOR THE AFOREMENTIONED COUNTRIES

European Legislation allows international transfer to the EU Member States.

The European Commission Resolutions 2000/18/CE, 2000/519/CE and 2000/520/CE included recognize and allows international transfer to the American organizations under Safe Harbor.

The Directive establishes that transfer to third countries may take place only if the third country in question ensures an adequate level of protection (Chapter IV European Directive).

In general terms personal data may be processed only in the following circumstances:

- When the data subject has unambiguously given his/her consent.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

The transfer made within the European Union implies that the company has to fulfill the law in each member state and the European Directive, which establishes that treatment of data must be included in a contract between the two companies including the following points:

- The processor shall act only on instructions from the controller,
- The processor shall implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. When a third party processes data, the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

Each company of the EADS Group has to be considered as a different company in terms of data treatment and transfer. That means that each company has to accomplish the legal requirements including the obligations of each Data Protection Law and sign the contract in the terms that have been explained.

If necessary, EADS entities will be responsible for reporting the transfer to the local Data Protection Agency according to their local legislation.

The principles that apply in view of international transfer of personal data are the following:

- Access to data will always depend on each user's assigned roles.
- Basic and medium level data may be transferred internationally among EADS Group entities.
- High level data will not be transferred among EADS Group entities