Replay Project

Gaming Technology Platform for Social Reintegration of Marginalised Youth

D3.1
Security Protocol for each Test Centre
D3.2
Process and Procedures for Informed Consent

Due Date: 31/08/2009 Release Date:12/10/2009

Circulation: PU

Responsible: AIJU
Compiled by: Sonia Torres
Partners: AIJU, White Loop, UAIC, LC, Rotalent

Table of Contents

Introduction

This document sets the minimum requirements to be met by each of the user centres participating in the Replay Project (Centro El Cerezo , Villena, Spain; Rotalent, Romania, Woolwich Polytechnic School, UK). All the centres have procedures that ensure that the Data Protection Laws of each country (Spain, UK and Romania) are respected, and these are normally more restrictive than that presented in this security document.

The security document presented here will ensure that the Data Protection Law is fulfilled in the least restrictive way possible, and so the document is as follows:

- A document with minimum requirements to be met by the future users of Replay.
- A good practice guide to follow for the countries in which the Data Protection Law is not a legal requirement.
- A procedure for the correct treatment of the information regarding personal data in each Replay user centre.

1.-Area of Application

1.1.- Area of Application

This Security Document is to be applied to the personal data that appears in the automated files that are described in the present document. It has been developed under the responsibility of the person that holds the legal title of Entity/Person Responsible for the File in the notification and inscription forms of the said files, presented before the General Register of Data Protection which has the responsibility, among others, of implementing and updating the Security Procedures that are detailed in this Document as well as ensuring their observance and updating.

All personnel with access to the protected data or to the information systems that enable their processing must observe all of the planned procedures. In these procedures all security measures, procedures and rules that must be adopted in order to guarantee the level of security required by Royal Decree considered in each country.

All of the people that are authorized to access the protected data –whether by means of an information system outfitted for access or by means of any other automated information system with access to the File or its data– are required by law to observe and obey what is established in the present Document and are also subject to the consequences that may come as a result of their non-compliance if such is the case. Every authorized person will receive a copy of this document or a copy of the part or parts that affect them, confirming the receipt of the said document being an obligatory requisite in order to be able to access that data.

According to what is stipulated by the Law, all persons or Companies that may be put in charge of processing the said data are also obligated to comply.

1.2.- Protection for Experimental Subjects

Ethical guidelines for the protection of human subjects will be based on guidelines and procedures already in place in the partner organizations. All psychological experiments will be conducted in compliance with EU ethical standards for experiments with human beings1 and

[1] *Ethics - The Ethical Review Procedure*. 2005;

with international ethical principles for running psychological experiments as described in the APA guidelines2.
Specific attention will be paid to the issues of privacy and data protection. Participants will be informed in detail about all aspects of the experiments relevant to these issues. An informed consent will have to be signed to ensure the information status of the subjects and their voluntarily participation. All experimental protocols will be approved by the local Human Investigation or Ethics Committees. Overall supervision of the experimental ethics will be the responsibility of the project ethics committee. The procedures and safeguards for specific experiments and trials are described below.

The files of personal data that will be generated in the playing sessions of Replay project will be handled and stored by the Schools or Re-education centres where the pilot playing sessions will take place. As described below, these centres are Centro de día El Cerezo- Villena (Spain), Rotalent- (Romania) and Woolwich Polytechnic School London (United Kingdom)

These centres will handle and store personal data following the security measures included in the Data Protection Directive. In line of these measures, these centres will ensure a "Security Document" as it is recommended in this report.

1.3.- Geographical Area and Location of the Files

Social Residence, the place where the activity is carried out and the physical location of the files in each country:

[Legal Organisation]
[Address]
[Telephone]
[Fax]
[e-mail]
[Website]

[2] *Ethical Principles of Psychologists and Code Of Conduct*. 2002; Available from: http://www.apa.org/ethics/code2002.pdf.

2.- Entity/Person Responsible for the File

2.1.- Responsiblefor the File

The Entity/Person Responsible for the File is:

[legal organisation] and [VAT number]
[address]

[Names of the legals representative] with the ID number [ID number], who holds the [position at the organisation] position and as the legal representative of the company Responsible for the File or Files described in an Annex, as stipulated in the National Organic Law regarding Personal Data Protection that approves the Security Measures Regulations of automated files that contain personal data, establishes by means of this Document the technical and organizing measures implemented in the described Company in order to guarantee the security, integrity and confidentiality of the information contained in the File or Files that contain personal data and, as such, are subject to the cited rules.

2.2.-Activity that is Carried Out

The activity carried out of the Entity/Person Responsible for the File is:
[Insert Activity]

2.3.-Function and Obligations

The principal functions and obligations of the Entity/Person Responsible for the File will be described in an Annex.

3.- Protected Files and Resources

3.1.-Types of Files

3.1.1.- Files that the Company Processes Directly

The automated files that contain personal data will be processed directly and solely by the Organisation with the responsibilities and security measures expected of the said organisation as the Entity/Person Responsible for the File.

3.1.2.- Files that the Company Releases to and Entity in Charge of Processing

In some cases the Organisation may release certain files to a third company (a professional consultant, outsourcing company, etc...) so that, this company, as an Entity in Charge of Processing, carries out the processing of certain technical processes such as: fiscal or mercantile declarations, the creation of payslips, massive issuing of documents (bills, receipts, etc...) and other similar operations.

The Company will verify that the Entity in Charge of Processing adopts the security measures prescribed in the National Security Measures Regulations so that the level of security corresponds to the typology of the data released for processing. The terms and conditions under which the said data is released must be established by means of a signed contract between the Entity/Person Responsible for the File and the Entity in Charge of Processing.

3.1.3.- Files that the Company Processes as an Entity in Charge of Processing for Third Parties

In other cases, the Organisation, as an Entity in Charge of Processing, carries out the processing of certain files, and the information contained therein, of third party companies.

The Company must adopt, as an Entity in Charge of Processing, the security measures prescribed in the National Security Measures Regulations so that the level of security corresponds to the typology of the data released for processing. The terms and conditions under which the said data is released must be established by means of a signed contract between the Entity/Person Responsible for the File and the Entity in Charge of Processing.

3.2.-Description of the Files

The files' description will be detailed in an Annex of this document as an integral part of the said document.
A file is "Any organized set of personal data, whatever the form or means of its creation, storage, organization and access may be". The Entity/Person Responsible for the File will be the one who determines its intended use, content and processing. The data to be recorded for each file is as follows:

- Name
- Description
- Principal Location
- Intended and Planned Uses
- Details on the Type of Information Collected
- Releasing and Communication or International Transfers
- Head of Security, if such a figure exists for the file in question
- Information Technology Applications or Programs that Process it
- Places or Locations where it is processed or accessed, name of the area, Department, etc…
- Operating Systems in which the file processing programs work
- Telematic Communications

Any file that may contain personal data must be identified with a code or abbreviated name that enables its identification and reference in other documents or annexes. If tests are carried out with real data, these test files will be listed, indicating the name and description of the said files and the planned procedure for the physical deletion of this data.

3.3.-Rights of Those Affected or Interested

3.3.1.- Information Rights

The people from whom personal data is solicited must be previously informed about the existence of a file or data processing, the intended use and the recipient of the information, the obligatory or optional nature of their response, the consequences of their submitting data or their refusal to supply it, the possibility of exercising access, cancellation and rectification rights and, finally, the identity and address of the person/entity in charge of processing. If questionnaires or other printed documents are used for collection, this information will appear

clearly and legibly in the said documents. The information rights clauses that the entity is using regarding the owners of the data will be also included in Annex to this document.

3.3.2.- ARCO (Access, Rectification and Cancellation by the Owners) Rights

Any person who is authorized to access and/or process the protected File's data must be familiar with and provide the rights that the current legislation assigns to those affected or interested, among those are the following:

In accordance with what is stipulated in the main National Personal Data Protection Law in Europe, access, rectification and cancellation rights must be provided to the owners of the personal data contained in the files.

4.- International Transfer of Data

4.1.-Rules

International transfers of data to European Union countries do not need the prior consent of the Director of the Data Protection Agency.
International transfers of data are at all times subject to the national laws, with special attention to the following:

- Information responsibility
- Express consent requirement
- Data recipient's obligation to observe all of the legal precepts and, specifically, apply the security measures and not carry out any later releasing of data without observing the legal requisites.
- Guarantee the data owner's rights at all times
- Observe the security measures planned in the National Royal Decree concerning data transmission.

The notification of files affected by the international transfer of data to the Data Protection Agency must include all of the data planned for this situation.
This section deserves special attention considering that the irregular releasing of data is a very serious matter.
The recipients of the said data transfers will be indicated.

4.2.-Encoded Transmission of REPLAY Data

The Centres in charge of handling personal data will dissociate the global data only transferring the data needed to develop technical activities in the project and hiding personal information and only working with codes.

Following this approach, the identifiable personal data will NOT be transferred among the Consortium members and so, it will NOT be necessary to apply either special regulation for international data transfer or for special contracts between of those responsible for the files in each centre and the rest of the Consortium members for data handling. Data transfer will be done only if previous informed consent has been given and previous encodement of identifiable data has been done.

5.- File Processing Centres

5.1.-Centres and Place of Work

The protection of data against unauthorized access and misuse must be established by means of the control, in turn, of all the ways in which the said data can be accessed.

The centres or facilities susceptible of being a direct or indirect means of access to the protected file must be controlled by these security rules.

The processing centres and places where the files are located or where the media that contains them is stored will all be listed in an Annex.

Access to the premises where the server that contains the files with protected data is located must be restricted exclusively to authorized personnel. All of the company's personnel must be warned of this restriction.

The mentioned annex must contain the following information and aspects:

- Location
- Distribution
- Departments or Workgroups
- Personnel authorized to access the facility
- Details of the access measures to the premises and restricted areas
- Activity or Activities carried out in the said premises

5.2.-Location of the Information Processing Systems

Regardless of the system chosen for the processing of information, the Organisation must take security measures regarding the access and availability of the components that make up the said system.

The rooms or premises where the information processing systems are located or where the media that contains the information is stored will have access restricted to only the personnel specifically authorized in an Annex.

Security measures, established in an Annex, will exist that, in the absence of personnel, guarantee the access and security of the components and information contained therein such as

an alarm or access detector, smoke detector or measures against fires or those that are considered appropriate and, as such, are specified in the said annex.

The premises where the computer or computers that contain the file are located must be the object of special protection that guarantees the availability and confidentiality of the protected data, especially if the File is located in a server accessed via a network. The description of the available means in each location will be included in an Annex to this document.

5.3.-Workplaces

These include all of the devices from which the File's data can be accessed such as, for example, terminals or personal computers.
Any location from which a user has access to the files' information, or processes it, must consider a series of additional measures applying to the users that have access to the said location, which guarantee the use of and access to information that they have at their disposal. These measures, will be dealt with in an
Annex.

System administration terminals are also considered workplaces such as, for example, the operating consoles where in some cases the file's protected data can also appear.
Each workplace will be under the responsibility of one of the people authorized, who will ensure that unauthorized people cannot see the information that is shown.
When the person responsible for a workplace leaves, whether momentarily or upon finishing their shift or workweek, they must leave it in such a state that impedes the protected data from being seen. This can be carried out using a screensaver that keeps the data from being seen. Resuming work will involve deactivating the screensaver by entering the corresponding password.

The monitors as well as the printers or any other type of device connected to the workplace must be physically located in places that guarantee this confidentiality.

Regarding the printers, it must be ensured that no documents containing protected information are left in the print tray just as documents should not be left in the print queue either. If the printers are shared with other users not authorized to access the File's data, those responsible for each workplace must pickup the documents as they are being printed.

Connecting to networks or systems outside of the workplace from which the files are accessed is strictly prohibited. The revocation of this prohibition will be authorized by the person responsible for the file, a record of this modification being kept in the Incident Register.
The workplaces from which access to the File is obtained will have a set configuration in its applications and operating systems that will only be able to be modified with authorization from the Head of Security or by the Administrator(s) authorized.

6.- Information Technology Equipment and Area

6.1.-Procesing Systems

Among the ways of accessing the information, special attention will be paid to the equipment and area of the information processing systems that the Company has at its disposal.

All of the components that make up the said information technology system or the information processing system will be described and detailed in an Annex. (Servers, Computers, Laptops, Printers, Hubs, Routers, etc…). In this annex the following information will appear for every one of these items:

- The component's internal code (the Company's numbering)
- Name of the component
- Type of component (computer, printer, SAI, Switch…)
- Description of the component
- Location or place of the component
- Workplaces with access to the component
- The intended use of the component
- The serial number if it has one
- The acquisition date
- The guarantee's expiration date
- The provider of the component
- The company in charge of maintenance
- The person inside of the Company in charge of the component
- Technical characteristics (if it is a computer then a list of details)
- The installed operating system (if it were a computer)
- The serial number of the operating system (if appropriate)
- The files that are processed in the component (if a server or computer)

6.2.-Operating Systems

The different components that make up the information technology system operate under some programs called operating systems that allow the said systems to interact with the components that are installed and other existing systems. These systems will be mentioned in the Annex with the following information:

- Name and Version

- Maker
- General Characteristics (single-user, multi-user, sharing, etc…)
- Access Control Characteristics
- Login Files and the Systems Own Recuperation Procedures
- Those Responsible for Maintenance

Although the established method for accessing the File's protected data is the information technology system referenced in the Annex, it is possible that people who know these areas can access the protected data without passing through the security procedures established in the application given that the file is located in a computer with a certain operating system and may be equipped with connections that allow it to communicate with other computers.

As such, these rules must regulate the use and the access of parts of the operating system, tools or utility programs or the communications area in such a way that unauthorized access to the file's data is impeded.

The File's operating and communications systems must have at least one Person Responsible that, as an Administrator, must be mentioned in an Annex.

In the simplest case, such as the file being located in a personal computer and accessed by means of a local, single-user application, the Operating System Administrator can be the person who normally accesses the File.
No tool or utility program that allows access to the File should be accessible to any user or administrator not authorized, including any indirect means of access to the data, in other words means not developed or edited, such as queries, universal editors, file analysers, etc… that must be under the control of the authorized administrators listed in the aforementioned Annex.

The Administrator must be responsible for saving the back-up copies of the file in a secure place in such a way that no unauthorized person has access to them.

If the File's access application or system usually uses temporary files, login files or any other means in which copies of the protected data could be made, the administrator must ensure that this data is not later accessible to unauthorized personnel.

If the computer in which the file is located is connected to a communications network in such a way it is possible to access the File from other computers connected to the same network, the

Administrator responsible for the system must ensure that this access is not given to unauthorized persons.

6.3.-Information Technology Programs and Applications

The information technology programs and applications used for accessing the data will be described in an Annex.
The information technology File access system or application is the set of programs specifically designed for this use or intention by means of which the File's data is normally accessed for consultation or updating.

These systems can be information technology systems specifically designed for accessing the File or pre-programmed, general-purpose systems such as applications or packages available on the information technology market.

The information technology File access systems must have their access restricted by means of a user code and password.

All of the users authorized to access the File, must have a user code that identifies them and that is associated with the corresponding password, which will only be known by the said user.

If the information technology application that allows access to the File does not have a built-in access control, the operating system where the application is executed must have one or use a specific application that impedes unauthorized access using the previously mentioned user codes and passwords.

In any case, fraudulent attempts at accessing the file will be controlled by limiting the number of unsuccessful login attempts and, when technically possible, by saving the date, time, code and erroneous passwords that have been entered in a specific register along with other relevant data that may help uncover who is behind these unauthorized access attempts.

If real data is used during the testing prior to the implementation or modification of the File access application, the same security procedures that are applied to the File must also be applied to these files, and these test files must be listed in an Annex.

For each access, at least the user's identification, the date, time at which it was carried out, the file accessed the type of access and if it has been authorized or denied will be saved. If the

access is authorized, the record's password or information that allows the identification of the record accessed will be saved.

The aforementioned information will be saved for a minimum of two years.
The description must at least contain the following data:

- Name of the application
- Whether a package or standard product on the market or some programs specifically designed for this use are being dealt with
- The person or company who has developed it
- Those responsible for maintenance
- Type of access control, if applicable, indicating if the number of failed access attempts is limited and if the history of these is attempts is saved in an auxiliary file.
- Type of operation (login) and recuperation tracking procedures if it has them.

7.- Functions and Obligations of the Personnel

7.1.-General Rules

The Company has adequately informed the employees about the security measures and rules that affect the carrying out of their functions, about the obligatory nature of complying with these rules as well as the consequences that could come about if they are not followed. The functions and obligations of the personnel will be described in an Annex. Nevertheless, the System Administrators must additionally abide by those more extensive and stricter rules that are mentioned in this Annex that deal with, among other things, the handling of security supports, rules for registering users and passwords as well as other rules that must be abided by in the department or section that the File belongs to.

7.2.-Affected Personnel

7.2.1.- Head of Security or Data Governance Officer

The general functions of the Head of Security will be the coordinating and controlling of the security measures described in this Security Document while, at the same time, being the link with the Person/Entity Responsible for the File. However, at no time shall this imply the delegation of the latter's responsibility to the former.
The Head of Security will appear, with an explicit mention of his/her post, in the list of personnel that will be attached to this Document as an Annex. His/her functions and obligations will be listed in the above mentioned Annex.

7.2.2.- Users of the File

This refers to the personnel that habitually use the information technology File access system. The Head of Security will assign those people with authorized access to protected places, resources and files for processing. These personnel will only be able to access the files authorized for them as will be reflected in an Annex.

7.2.3.- Systems Administrators

The System Administrators are those in charge of administrating or maintaining the File's operative area. These personnel must be clearly listed in an Annex since, due to their functions; they can use administrative tools that give them access to the protected data, bypassing the application's access barriers. Their functions and obligations will be described in the same Annex.

7.3.-General Obligations of the Personnel

The personnel will maintain absolute confidentiality about the files' data and in no event will they carry out any kind of processing different from that which is described in this Document. They will also act in accordance with the rules that are described in the present document.

They will also report any incident that comes about while processing the files to the Head of Security.

The personnel authorized to intervene in the processing of personal data files will be conveniently informed about the principles of data protection regarding the fundamental aspects that the personnel must respect with reference to:

1. The quality, veracity and exactness of the data
2. Information rights in the collection of data, whenever applicable
3. The consent of those affected, whenever it is applicable
4. Especially protected data
5. Data security

7.3.1.- Receiving Requests

The Person/Entity Responsible for the File, or in their place the Entity in Charge of Processing, must attend to the requests of the owners of the personal data in the files if they demand the data access, rectification or cancellation rights granted to them by the Law. If the demand is forthcoming, the Person/Entity Responsible for the File and/or the Entity in Charge of Processing, will give instructions to the Head of Security so that the latter carries out the corresponding actions in order to attend to the data owner's request, inside of the time period that is set by the DPOL (Data Protection Organic Law) and in accordance with the procedures that are specified in the following points.

If an authorized User or the Head of Security receives the request of the affected party, they will pass on the request to the Person/Entity Responsible for the File or the Entity in Charge of Processing as soon as possible so that they can act accordingly.

When the Person/Entity Responsible for the File or the Entity in Charge of Processing notifies the Head of Security about the authorization for the owner of data in a file to exercise his/her rights recognized by the Law (access, rectification or cancellation), the Head of Security will have the necessary measures at his/her disposal to act as indicated in the next three points.

7.3.2.- Right of Access

According to the circumstances, the Head of Security will determine if the affected party will exercise their rights by means of viewing the said data or if the said data will be given to them in a printed document. In any case, a record of this will be kept in the incident register.

7.3.3.- Right of Rectification

When the Person/Entity Responsible for the File or the Entity in Charge of Processing has determined that the data is not correct, the Head of Security will directly carry out their rectification or will arrange it to be carried out by the User authorized to access the said file. A record of the rectification must be kept in the incident register.

7.3.4.- Right of Cancellation

The Person/Entity Responsible for the File or the Entity in Charge of Processing will have previously determined if the data to be cancelled can be requested by the Public Service. If such is the case, the Head of Security will have what is necessary at his/her disposal so that this information is blocked in the devices with data processing applications until the legal time period has expired. If the opposite is the case, the Head of Security will destroy the data directly or ensure that it is carried out punctually by a User authorized to process the affected file.

Any cancellation of data must be recorded in the incident register.

Everyone has been given a copy of the Security Procedures Manual that includes the legal data protection principles and the principal measures and procedures implemented by the Company to guarantee the security of the said data.

8.- Paper Documentation

During the course of the Files' creation, maintenance or processing, we will surely have to use written documents in paper format that contain personal data, the Personal Data Protection Law also applies to these documents.

When dealing with paper documents the following procedures will be followed:

1. They will only be able to be processed by authorized users
2. After being received and processed, the authorized user will do the following:
    a. If a document containing variable data is being dealt with, it will be destroyed
    b. The user will also destroy any written notes that contain person data provided that their conservation is not necessary.

If the document must be saved, it will be stored in a physical file in a place not accessible to the public and in a locked closet. The key will be held by the Head of Security, and access to this closet will be restricted to authorized users.

9.- Administration of Media

9.1.-Definition

Information technology media is any means of data recording and recuperation that is used to carry out the making of copies or intermediary steps in the File administration application's processes.

Given that the majority of the media used today, such as disks or CD-ROMs, is easily transportable, reproducible and/or able to be copied, the importance of having control of this media for the security of the data in the files is evident.

9.2.-Inventory, Identification, Storage, Reusing and Unfitness

The Head of Security will keep a carefully labelled Media Inventory.
The media that contains the File's data, whether a consequence of the processing application's intermediary operations, a consequence of periodic back-up procedures or any other sporadic operation, must be clearly labelled with an external sticker that indicates what file is being deal with, what type of data it contains, the process that has created it and its date of creation.

This media must be stored in places that people not authorized to use the file cannot access and, if possible, in a locked closet. The key will be held by the Head of Security.

Any media that can be reused, and that has held copies of the protected File's data, must be physically deleted before reusing in such a way that the previously contained data can't be recuperated. The media that has been subjected to a process of physical deletion must be identified. If any media should result unfit for use, it must be physically destroyed in neither such a way that it cannot be used later nor any data that it may have contained be recuperated.

9.3.-Movements and Distribution of Media

The Head of Security will keep an Incoming and Outgoing Media Register where the forms, created to this end and listed in Annex, will be saved, indicating the following:

- Type of Media
- Date and Time of Receipt/Sending
- Issuer
- Amount of Media
- Type of Information Contained

- Method of Sending
- Recipient/Destination

The sending of any information technology media that contains the File's data outside of premises where the said File is located must be clearly authorized by the Person/Entity Responsible for the File, using an appropriate to this end.

When the media must be sent outside of the premises where the File is located in order to carry out maintenance operations, according to each case and/or circumstance, the Authorized User, with the consent and approval of the Head of Security, will adopt the appropriate measures to impede any type of unauthorized recuperation of the stored data.

If the transportation of media with personal data from a confidential file is necessary, its security level being MEDIUM and/or HIGH, the Head of Security will establish the necessary technical procedures to encode the information, or similar technical measures, in order to impede the recuperation and/or alteration of the data.

10.- Telecommunications

The transmission of data over the Internet, whether it is via E-mail or by means of a file transfer system, is becoming one of the most utilized means for the sending of data to such a degree that it is replacing physical media. As such, they deserve special treatment given that, because of their characteristics, they can be more vulnerable than traditional physical media.

In order to provide the necessary security measures for the reasonable protection of the transmitted data, this document establishes the following measures:

- All sending and receiving of the File's data that is done via E-mail will be carried out from a single account or E-mail address controlled by a user specially authorized by the Person/Entity Responsible for the File. Similarly, if the sending or receiving of data is carried out by means of a file transfer system over the Internet, only the Enabled User or the System Administrator will be authorized to carry out the said operations.

- Copies of all the E-mails that involve the sending or receiving of the file's data will be saved in protected directories under the control of the Head of Security.
Copies of those E-mails will be kept for at least two years. During the same time period, copies of the files received or sent via file transfer systems over the Internet will also saved in protected directories along with a record of the date and time at which the operation was carried out and the destination of the sent file.

- When the File's data is going to be sent via E-mail or file transfer systems, by means of public or non-protected networks, it must be encrypted in such a way that it can only be read and interpreted by the recipient.
The possibility of different information technology elements communicating with others inside or outside of the system will be carried out through of a means of communication. The different types of communication established inside, towards or from the outside should be listed in an Annex including the following information:
  - Type of local network (Ethernet, others), area and extension
  - If a connection with other local networks or a WAN exists, indicate the type of Connection (permanent, sporadic, etc…), by means of public networks such as the Internet or private connections, etc…
  - File and Resource Sharing. Indicate the type of network system that is used, its limits and reach.
  - Access controls between the network and the File's System

11.- Data Encoding Systems

The encoding system is a security measure used in the transmission of data. The Person/Entity Responsible for the File will decide to implement security measures that prevent unauthorized access to the information contained in the different databases. Similarly, measures that impede the reading of the information's content during travel outside of the premises via telematic means will be obligatorily determined. Highly classified information encoding or encryption systems will also be implemented when it is sent via telematic means. These measures are must be described with the following information detailed:

- System, method or name of the program used to encode the files
- Maker
- Version
- Characteristics of the encoding method
- The person responsible for the encoded file register
- Authorization
- Motive
- Types of files to encode
- Procedure

12.- Back-Up and Recuperation Copies

The security of the File's personal data not only implies confidentiality regarding the said data but also their integrity and availability as well. In order to guarantee these two fundamental security aspects, the existence of back-up and recuperation procedures is necessary that, in case of the information technology system's failure, allow the recuperation and possible reconstruction of the File's data.

The Person/Entity Responsible for the File will designate a person, be it a System Administrator, a User or the Head of Security, to assume the responsibility of periodically obtaining a back-up copy of the file, for the backing-up and possible recuperation in case of failure.

These copies must be carried out periodically, at least weekly, except if no change in the data has occurred.
If system failure occurs with the complete or partial loss of the File's data, an information technology or manual procedure will exist that, based on the last back-up copy and on the record of operations carried out since the last back-up, reconstructs the File's data, returning it to the state that it was in at the moment of failure.

The written authorization of the Person/Entity in Responsible for the File or the Entity in Charge of Processing will be necessary for the execution of the data recuperation procedures. A record of the changes that have been necessary to carry out the said recuperations must be kept in the incident register, including the identification of the person who carried out the process, the restored data and the lost data, provided that their identification is possible and that the data has been manually recorded during the recuperation process.

The Head of Security must keep the copies and must also save a back-up copy and a copy of the data recuperation procedures in place other than where the information technology data processing equipment is stored. In the said place, the necessary security measures must be installed in order to protect the mentioned copies from any possible risk.

13.- Password Assignement Procedures

13.1.-The Safeguarding and Protection of Personal Passwords

Personal passwords constitute one of the basic components of data security and, as such, must be especially protected. As access keys to the system and programs, the passwords must be strictly confidential and personal, and any incident that compromises their confidentiality must be immediately communicated to the Head of Security or authorized System Administrator, corrected as soon as possible and recorded in the incident register.

Only the authorised people will be able to have access to the File's data.

Each user will be responsible for the confidentiality of their password, and if it is accidentally or fraudulently discovered by unauthorized persons, it must be recorded as an incident in the Incident Register, just as it is specified in Annex, before proceeding immediately to replacing it.

The passwords will be assigned and will be changed by means of the mechanism and time period that will be determined in an Annex.
The user codes and passwords will be stored encoded and unintelligible, and the file where the said passwords are stored must be protected and be under the responsibility of the Head of Security or the System Administrator.

The Head of Security must review the access register at least once month and write a report with the detected incidents that will be saved and classified chronologically.

14.- Administration of the File Access Register

The Person/Entity Responsible for the File will ensure the implementation of those precise technical measures for the creation and maintenance of an updated register of the accesses to the protected files carried out by the authorized users.

A record of the accesses will be kept for two years in the way determined by the Person/Entity Responsible for the File.
The mechanisms that permit the recording of the data detailed in the previous paragraphs will be under the control of the Head of Security, without ever allowing the deactivation of the said mechanisms.

The information that this register must contain will be:
- Identification of the User
- Date and Time of Access
- The File Accessed

Another register will also accompany this one, with the same information as the previous one, regarding the unauthorized access attempts or those denied by the system.
The Head of Security will be in charge of periodically reviewing the recorded security information and, at least once a month, will write a report about the reviews carried out and the problems detected.
The procedure employed should be described in detail in an Annex.

15.- Administration of Incidents

An incident is any event that can come about sporadically and that can pose a danger to the File's security, as understood under the aspects of confidentiality, integrity and data availability.

Keeping a record of the incidents that compromise the security of a File is a necessary tool for the prevention of possible attacks, as well as for the prosecution of those responsible for the said attacks.

Moreover, from the analysis of the incidents we can establish its causes and adapt our security system to prevent its repetition.

The Head of the File's Security will have an Incident Register available to all of the File's Users and Administrators in order that they record in it any incident that could pose a danger to the said file. Any user that has knowledge of an incident is responsible for recording the said incident in the Incident

Register or, if such is the case, communicating it, in writing, to the Head of Security or the Person/Entity Responsible for the File within twenty-four hours of being detected.
A user having knowledge of and not notifying about or recording an incident will be considered a security breach on the part of that user.

The notification or recording of an incident must include at least the following information:
- Type of Incident
- Date and Time at which it happened
- Person who is carrying out the notification
- Person to whom it is communicated
- Effects that could result
- Detailed Description of the said incident

The Head of Security will immediately act in order to adequately respond to the incident, taking the pertinent measures regarding the case and/or proposing the most appropriate actions for its prevention to the Person/Entity Responsible for the File and/or the Entity in Charge of Processing, including the modification or expansion of the security measures described in this Document.

The procedure employed should be described in detail in an Annex.

16.- Periodic Security Checks

With the intention of systematizing the control of the security measures described in this document, their usefulness, the veracity of the data reflected and the level of compliance, a series of methodical checks are established that the Head of Security must periodically carry out in accordance with the time periods described below. All of this takes place regardless of the other procedures, technical security measures and attitudes of the personnel that are involved in the rest of the controls, prescriptions and rules.

16.1.-Weekly Checks

The creation of back-up copies and their adequate processing will be checked weekly.

16.2.-Monthly Checks

Each month, the System Administrators or the person in charge of the information technology maintenance must inform the Head of Security about the modifications or alterations of the elements that make up the said system and that are included in the corresponding annexes of this Document, specifically about:
- File additions, modifications or removal
- Information Technology System additions, modifications or removal
- Additions, modifications or removal of personnel authorized to access the files

The updating of this Document will be undertaken according to the said modifications.
The Head of Security will also check monthly that the list of authorized users that appears in the Annex corresponds to the list of the users actually authorized in the File access application. This inspection is not related to the obligation that exists to inform the Head of Security of any addition or removal of users with authorized accessed to the file as soon as it happens.

The Head of Security will review monthly the recorded inspection information and will write a report on each of these reviews and the problems and incidents detected.

16.3.-Trimester Checks

At least once every three months, compliance with what is planned in sections 9 and 10 of this Document will be verified, regarding the sending / receiving of data, whether it be via the Internet or magnetic media.

The Person/Entity Responsible for the File and the Head of Security will analyse every trimester the latter's reports and the incident annotations recorded in the register in order to adopt, regardless of the measures adopted in the moment that the incident occurred, the corrective measures that allow the said incidents to be avoided or limit their occurrence in the future.

16.4.-Semesters Checks

Six months after the implementation of the Information Technology System's Security Measures, the changing of authorized user's passwords and the updating of the corresponding register will be carried out. The mechanisms that allow the monitoring of accesses will be under the direct control of the Head of Security without ever allowing the deactivation of the said mechanisms, except by a higher power and always with his/her knowledge and previous consent.

16.5.-Annual Checks

Annually, a general review of the files, information technology resources, authorized users and applied security systems will be carried out with the intention of detecting possible malfunctions or the obsoleteness of any of the adopted measures or formal requirements planned by the legislation in effect at each moment. It is recommended that this check be carried out by contracting outside resources that can provide an objective analysis of each and every one of the analysable aspects with the participation of those internally responsible when necessary.

When this review is finished, the drafting of a detailed report will be proceeded to, which will be given to the Head of Security, who will subsequently present it to the Person/Entity Responsible for the File so that he may have precise knowledge of the state and validity of the security system.

This review prepares and facilitates the audit planned in the current legislation, which must be carried out at least biannually in those cases where it is applied.
It is recommended that this revision be entrusted to external qualified personnel.

17.- Audits

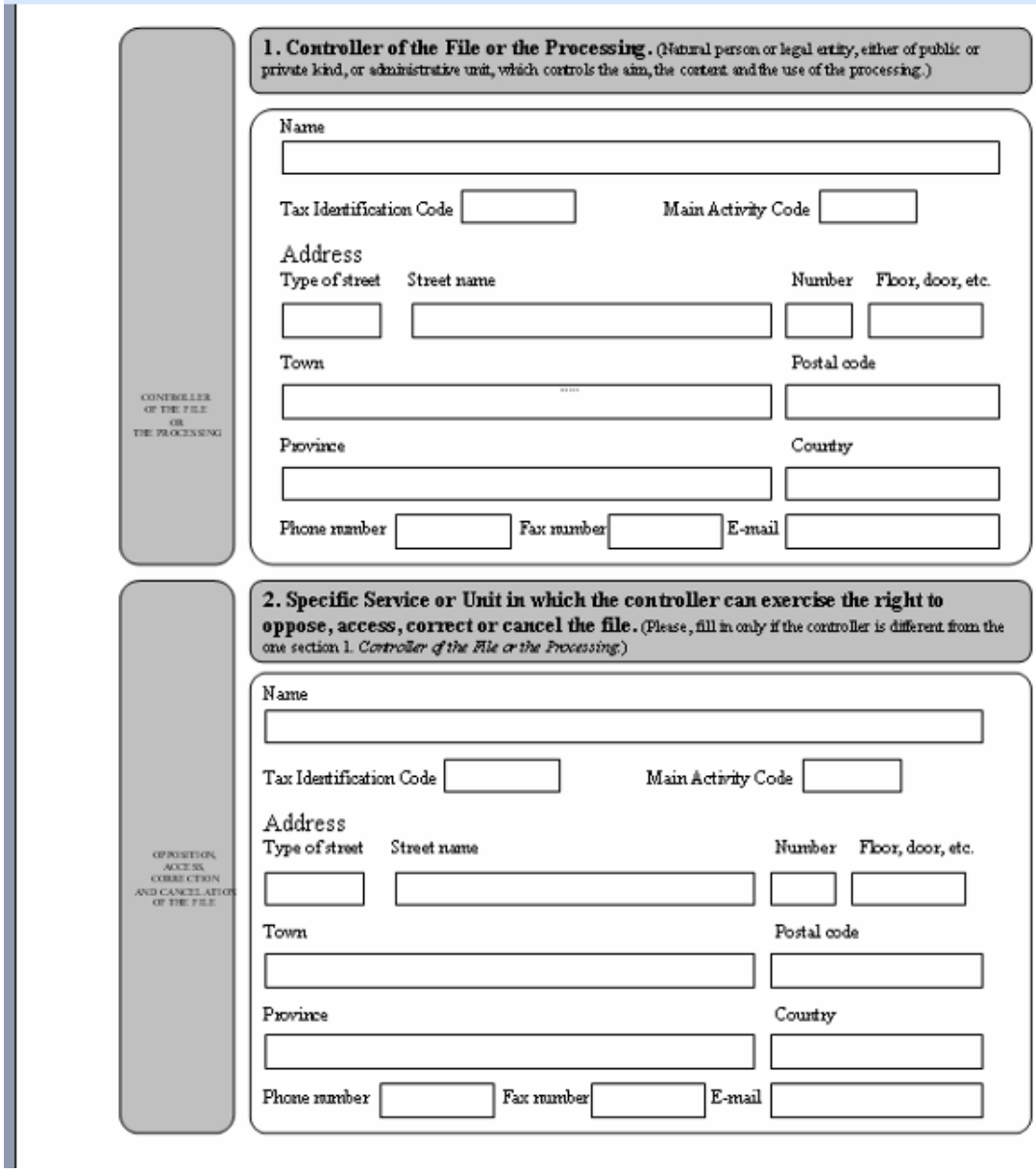
Every two years, all of the information and procedural systems, as well as the compliance with the rules and procedures described in this Document, will be audited.

The said Audit can be carried out by external or internal resources, the latter option being recommended.

It must allow the exact situation of the correct compliance with and the suitability of the security measures planned in this Document and in the current rules to be known, indicating the weak points, deficiencies and possible non-fulfilments and proposing the necessary corrective measures.

After each Audit, a report must be written that will be analysed by the Head of Security, who will subsequently propose the necessary corrective measures to the Person/Entity Responsible for the File.

18.- Annex: Example of form for registering



1. Controller of the File or the Processing. (Natural person or legal entity, either of public or private kind, or administrative unit, which controls the aim, the content and the use of the processing.)

CONTROLLER OF THE FILE OR THE PROCESSING

Name

Tax Identification Code | Main Activity Code

Address

Type of street | Street name | Number | Floor, door, etc.

Town | Postal code

Province | Country

Phone number | Fax number | E-mail

2. Specific Service or Unit in which the controller can exercise the right to oppose, access, correct or cancel the file. (Please, fill in only if the controller is different from the one section 1. *Controller of the File or the Processing.*)

OPPOSITION, ACCESS, CORRECTION AND CANCELLATION OF THE FILE

Name

Tax Identification Code | Main Activity Code

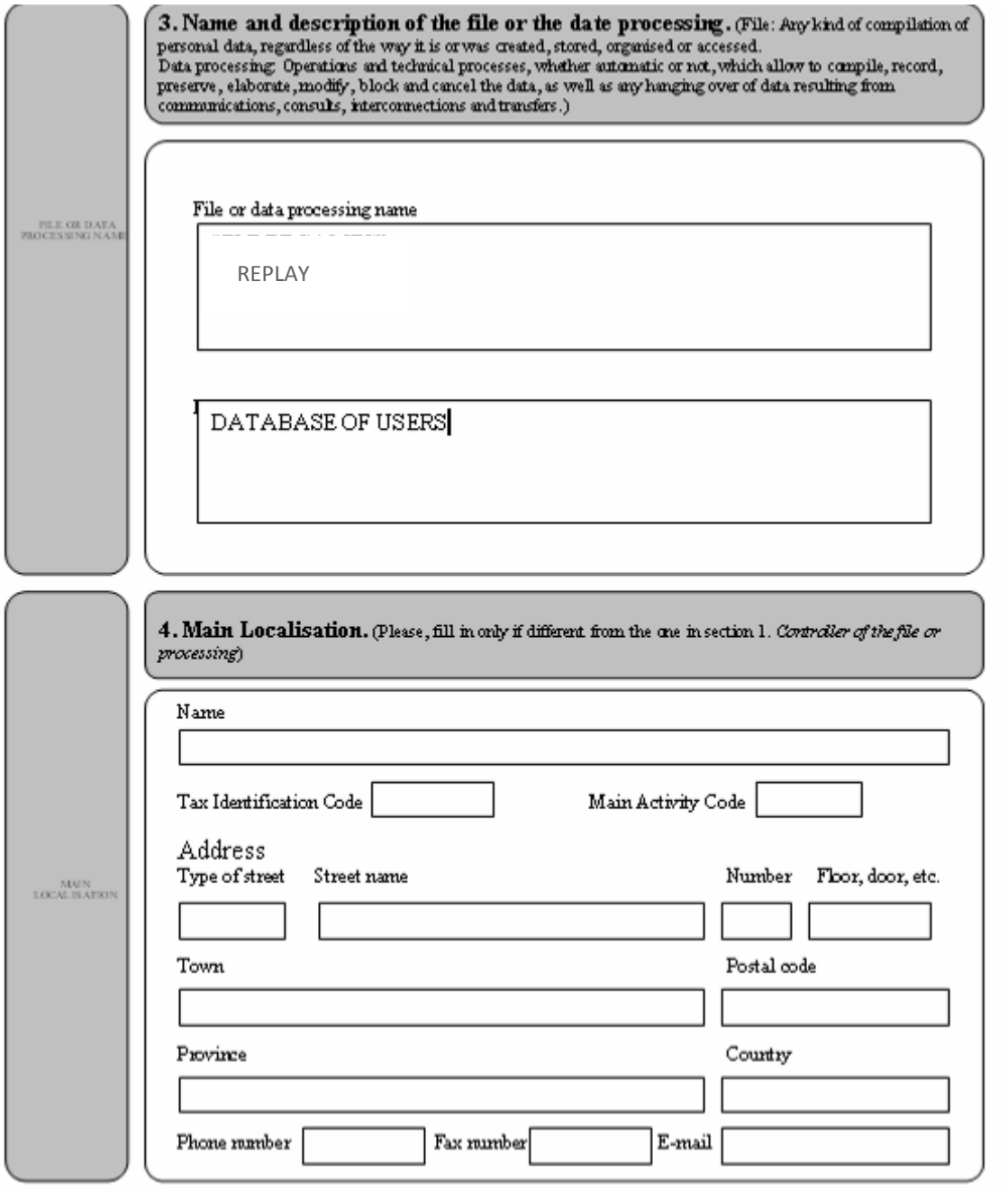
Address

Type of street | Street name | Number | Floor, door, etc.

Town | Postal code

Province | Country

Phone number | Fax number | E-mail



3. Name and description of the file or the date processing. (File: Any kind of compilation of personal data, regardless of the way it is or was created, stored, organised or accessed.
Data processing: Operations and technical processes, whether automatic or not, which allow to compile, record, preserve, elaborate, modify, block and cancel the data, as well as any hanging over of data resulting from communications, consults, interconnections and transfers.)

FILE OR DATA PROCESSING NAME

File or data processing name

REPLAY

DATABASE OF USERS

4. Main Localisation. (Please, fill in only if different from the one in section 1. *Controller of the file or processing*)

MAIN LOCALISATION

Name

Tax Identification Code | Main Activity Code

Address

Type of street | Street name | Number | Floor, door, etc.

Town | Postal code

Province | Country

Phone number | Fax number | E-mail

CONTROLLER OF THE DATA PROCESSING

5.Controller of the Processing. (Natural person or legal entity, public authority, unit or any other organism, on its own or together with others, processes personal data for the controller of the file or the processing). Please, fill in only when a third party carries out the processing for the controller.

Name

Tax Identification Code | Main Activity Code

Address

Type of street | Street name | Number | Floor, door, etc.

Town | Postal code

Province | Country

Phone number | Fax number | E-mail

PROCESSING SYSTEM

6. Information or Processing System. (Group of files, programmes, supports and equipments used to store and process personal data.

Overall description of the information system

CENTRAL SERVERS
PERSONAL COMPUTERS
OTHERS

Are there any other remote connections? NO YES
Type

In case of a web page, please write down the URL

SAFETY MEASURES

7. Safety measures.

The level of the safety measures adopted is

Low Medium High

BASIC STRUCTURE

8. Basic structure and description of the type of personal data included in the file.

Specially protected data

IDEOLOGY
UNION MEMBERSHIP
RELIGION
BELIEFS

Were these date collected with the specific consent of the target?
YES NO

Is the file maintained by any political party, union, church, confession o religious community, association, foundation or other non-profit entity, whose **aim** is political, philosophical, religious or related to a trade union in relation to their members?
YES NO

Other specifically protected data
RACIAL OR ETHNIC ORIGIN
HEALTH
SEXUAL LIFE

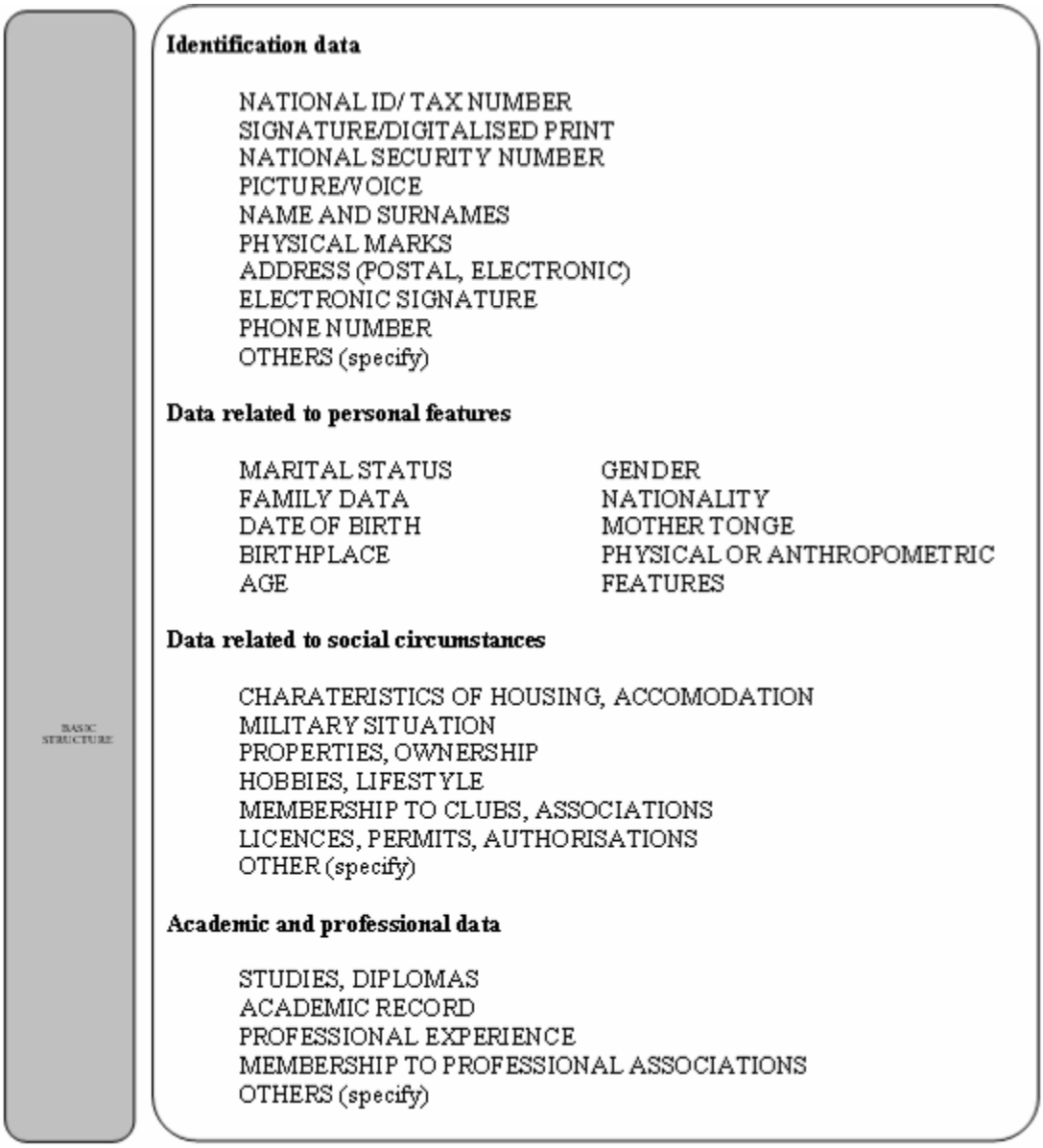
Were these date collected with the specific consent of the target?
YES NO

Is there any low which entitles the collection, processing and handing out of these data for general interest reasons?
YES NO

If the answer to this last question was YES, please specify what law releases the controller from the need to have the target's specific consent.

Law title **Law number** **Year**

LEY DE LA SEGURIDAD SOCIAL (Social Security Law)


BASIC STRUCTURE
Identification data
NATIONAL ID/ TAX NUMBER
SIGNATURE/DIGITALISED PRINT
NATIONAL SECURITY NUMBER
PICTURE/VOICE
NAME AND SURNAMES
PHYSICAL MARKS
ADDRESS (POSTAL, ELECTRONIC)
ELECTRONIC SIGNATURE
PHONE NUMBER
OTHERS (specify)
Data related to personal features
MARITAL STATUS
FAMILY DATA
DATE OF BIRTH
BIRTHPLACE
AGE
GENDER
NATIONALITY
MOTHER TONGE
PHYSICAL OR ANTHROPOMETRIC FEATURES
Data related to social circumstances
CHARATERISTICS OF HOUSING, ACCOMODATION
MILITARY SITUATION
PROPERTIES, OWNERSHIP
HOBBIES, LIFESTYLE
MEMBERSHIP TO CLUBS, ASSOCIATIONS
LICENCES, PERMITS, AUTHORISATIONS
OTHER (specify)
Academic and professional data
STUDIES, DIPLOMAS
ACADEMIC RECORD
PROFESSIONAL EXPERIENCE
MEMBERSHIP TO PROFESSIONAL ASSOCIATIONS
OTHERS (specify)

BASIC STRUCTURE

Data related to the job details

OCCUPATION
PREVIOUS JOBS
NON-ECONOMICAL DATA ABOUT THE SALARY
OTHERS (specify)

Commercial information data

ACTIVITIES AND BUSINESS
COMMERCIAL LICENCES
SUBSCRIPTION TO PUBLICATIONS/MEDIA
ARTISTIC, LITERARY, CIENTIFIC OR TECHNICAL CREATIONS
OTHERS (specify)

Assurance, economic and financial data

EARNED INCOME
INVERSION, PROPERTIES
CREDITS, LOANS, ENDORSEMENTS
BANK DATA
PENSION PLANS, RETIREMENT
ECONOMICAL DATA FROM SALARY
IMPOSITIVE/TAX DEDUCTION
ASSURANCES
MORTGAGES
ALLOWANCES, BENEFITS
CREDIT HISTORY
CREDIT CARDS
OTHERS (specify)

Transactional data

GOODS AND SERVICES PROVIDED BY TARGET
GOODS AND SERVICES RECEIVED BY TARGET
FINANCIAL TRANSACTIONS
COMPENSATIONS/INDEMNITIES
OTHERS (specify)

AIM OF THE FILE AND ITS PLANNED USES

9. Aim of the File and its planned uses.

9.a) Detailed description of the aim and its planned uses

PREPARATION OF SALARIES AND CONTRIBUTION TO SOCIAL SECURITY

9.b) Different types corresponding to the aim and uses

ACCOUNTANT, FISCAL AND ADMINISTRATIVE MANAGEMENT
ECONOMICAL AND ACCOUNTING MANAGEMENT
FISCAL MANAGEMENT
ADMINISTRATIVE MANAGEMENT
INVOICING MANAGEMENT
CLIENT MANAGEMENT
SUPPLIER MANAGEMENT
CASHING AND PAYMENT MANAGEMENT
REAL ESTATE MANAGEMENT
CONSULTANCY, AUTHORING, CONSULTING, RELATED SERVICES
HISTORY OF COMMERCIAL RELATIONS

HUMAN RESOURCES
PERSONNEL MANAGEMENT
SALARY MANAGEMENT
PERSONNEL TRAINING
SOCIAL ALLOWANCES
SELECTION OF PERSONNEL
TEMPORARY WORK MANAGEMENT
WORK PROMOTION AND MANAGEMENT
PREVENTION OF OCCUPATIONAL RISKS
TIME CONTROL

FINANCIAL-ECONOMICAL SERVICES AND ASSURANCES
CREDIT ACCOUNT
SAVING ACCOUNT
PROPERTY MANAGEMENT
PENSION MANAGEMENT AND SIMILAR
CREDIT CARD MANAGEMENT AND SIMILAR
REGISTER OF SHARES AND DEBENTURES
OTHER FINANCIAL SERVICES
FULFILMENT/NO-FULFILMENT OF MONEY DEBENTURES
PROPERTY AND CREDIT SOLVENCY SERVICES
LIFE AND HEALTH ASSURANCE
OTHER TYPE OF ASSURANCES

ADVERTISING AND COMMERCIAL RESEARCH

ADVERTISING
DISTANT SELLING
PUBLIC-OPINION POLLS
PROFILE ANALYSIS
COMMERCIAL RESEARCH
MARKET SEGMENTATION
DECISION-MAKING HELP SYSTEM
ADDRESS COMPILATION

TELECOMMUNICATION SERVICES

PROVISION OF TELECOMMUNICATION SERVICES
GUIDES OF TELECOMMUNICATION SERVICES
ELECTRONIC TRADE
PROVISION OF CERTIFICATION SERVICES

ASSOCIATIVE, CULTURAL, LEISURE, SPORT AND SOCIAL ACTIVITIES

MANAGEMENT OF CULTURAL ACTIVITIES
MANAGEMENT OF CLUBS OR SPORT, CULTURAL, PROFESSIONAL OR SIMILAR ASSOCIATIONS
MANAGEMENT OF MEMBERS OF POLITICAL PARTIES, TRADE UNIONS, CONFESSIONS OR RELIGIOUS COMMUNITIES AND ASSOCIATIONS, FOUNDATIONS AND OTHER NON-PROFIT ENTITIES
DIVERSE ASSOCIATIVE ACTIVITIES
SOCIAL WORK
MANAGEMENT OF SOCIAL MEDIA

EDUCATION

PRIMARY EDUCATION
SECONDARY EDUCATION
UNIVERSITY
SPECIAL EDUCATION
OTHER EDUCATIONS

HEALTH

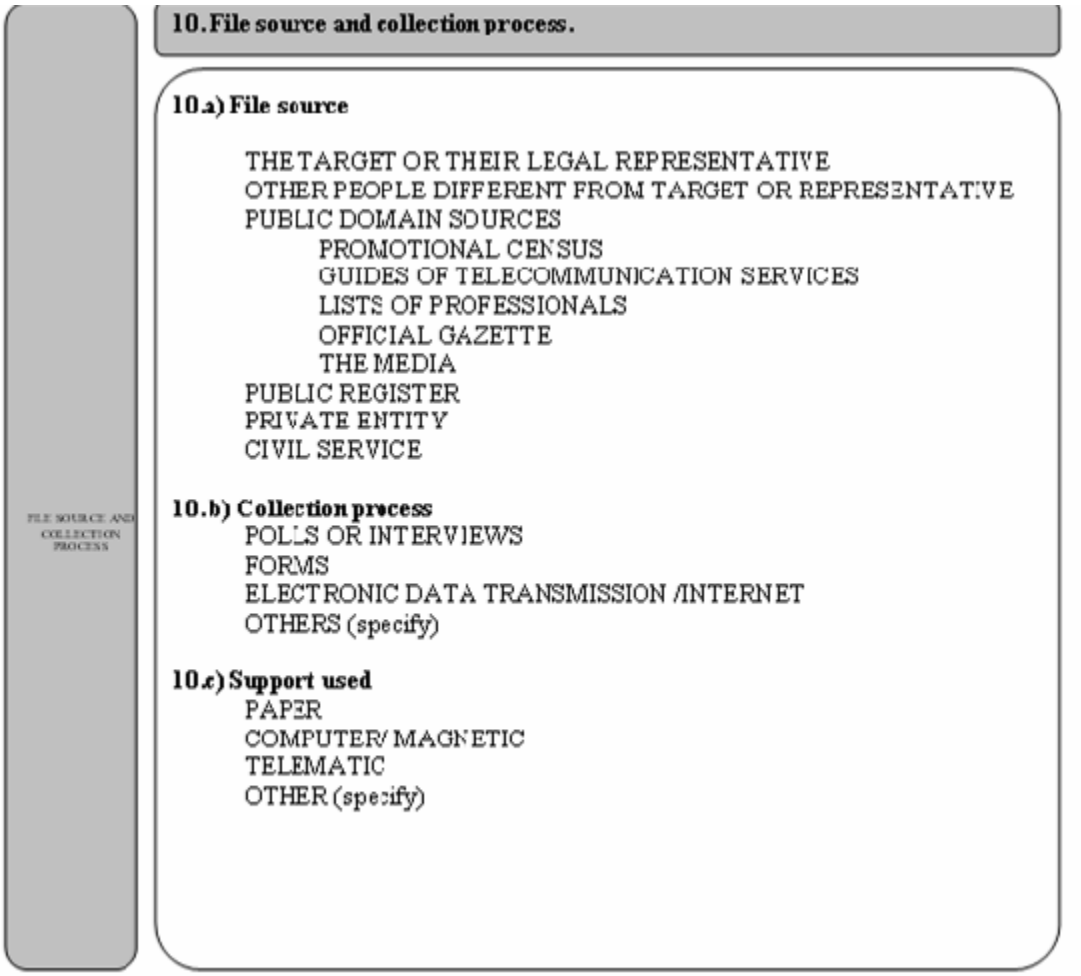
HEALTH CONTROL AND MANAGEMENT
PATIENT RECORD
EPIDEMIC RESEARCH AND SIMILAR ACTIVITIES

SECURITY

PRIVATE INVESTIGATION OF PEOPLE
SECURITY AND CONTROL OF ACCESS TO BUILDINGS
OTHER SECURITY ACTIVITIES

OTHER AIMS

CLIENT LOYALTY-MAKING
BOOKING AND ISSUEING OF TRAVELING TICKETS
HISTORICAL, SCIENTIFIC OR STATISTICAL AIMS


FILE SOURCE AND COLLECTION PROCESS
10. File source and collection process.
10.a) File source
THE TARGET OR THEIR LEGAL REPRESENTATIVE
OTHER PEOPLE DIFFERENT FROM TARGET OR REPRESENTATIVE
PUBLIC DOMAIN SOURCES
PROMOTIONAL CENSUS
GUIDES OF TELECOMMUNICATION SERVICES
LISTS OF PROFESSIONALS
OFFICIAL GAZETTE
THE MEDIA
PUBLIC REGISTER
PRIVATE ENTITY
CIVIL SERVICE
10.b) Collection process
POLLS OR INTERVIEWS
FORMS
ELECTRONIC DATA TRANSMISSION /INTERNET
OTHERS (specify)
10.c) Support used
PAPER
COMPUTER/ MAGNETIC
TELEMATIC
OTHER (specify)

HOLDER'S TAX IDENTIFICATION CODE:

AIM OF THE FILE AND ITS PLANNED USES

11. Cession or communication of data. (Referring to any transmission of data to any person which is not the target. Please, fill in case of a possible cession.

11.a) Cases in which data communication or cession is allowed

Do targets allow for it?	YES	
Are the data form public domain sources?		NO
Is the data processing carried out on a free and legitimate basis with regards to a legal relation which, when carried out, implies the compulsory communication of the data to third parties?		NO
Is there any law that allow it?	YES	

In case there is, please, specify the law:

Law number 1 **Year 1994**

LEY DE LA SEGURIDAD SOCIAL (Social Security Law)

11.b) Addressee of the cession or communication

TAX ID NUMBER/TAX ID CODE **NAME, ORGANISM**

Other specific addressee

INSS (INSTITUTO NACIONAL DE LA SEGURIDAD SOCIAL)
(National Institute for Social Security)

In case of determinable addressee o categories of addressees, please specify the rules that allow identification.

HOLDER'S TAX IDENTIFICATION CODE:

INTERNATIONAL TRANSFERENCE

12. International data transferences.

12.a) Legal cases in which it is allowed to carry out an international data transfer
(Of the international data transference does not match any of the following cases, you should ask for specific authorisation of the Head of the Data Protection Agency.

Is the transference towards countries with similar level of protection?	YES	NO
Is the transference the result of agreements signed by Spain?	YES	NO
Is it carried out to provide or ask for international legal help?	YES	NO
Is it needed for preventions or medical diagnose, the provision of medical assistance or medical treatment or the management or health services? Did the target allow for it?	YES	NO
Is it needed for the execution of a contract between the target and the controller of the file or to carry out pre-contractual measures agreed with the target?	YES	NO
Is it needed for the execution of a contract, favourable to the target, by the controller of the file or a third party?	YES	NO
Is it legally demanded to safeguard a public interest?	YES	NO
Is it needed to acknowledge, exercise or defend any right in a legal process?	YES	NO
Is it carried out, asked by the legitimate person, from a Public Register and does it match its aim?	YES	NO

12.b) Transference addressees

Country Name

Other specific addressees

In case of determinable addressee o categories of addressees, please specify the rules that allow identification.

HOLDER'S TAX IDENTIFICATION CODE:

DELETION

13 Deletion of the File inscription

Inscription code assigned by the Agency

Reasons for deletion

Destination of the information or measures considered for destruction

CHANGE

14. Change of the inscription of the file

Inscription code assigned by the Agency

Sections to be modified

Controller of the file or the processing
Service or unit where anyone can exercise their right to oppose, access, change and cancel the file
Name and description of the file or data processing
Physical localisation of the file
Controller of the processing
Processing system
Security measures
Basic structure and description of the type of data
Aim of the file and its planned uses
Source and process of data collection
Cession or communication of data
International data transferences

19.- Annex: Example of Confidentiality Statement (El Cerezo)

"El Cerezo center" acknowledges that it has a responsibility to members, staff and volunteers with regard to personal information that is held about them and has therefore adopted the following confidentiality policy:-

1. For the purposes of this policy confidentiality will be seen as an agreement to share information under strictly set rules. That is, no information provided by any member, staff or volunteer shall be passed to any other person without the express permission of the member, staff or volunteer concerned.

2. Only information that is necessary will be collected on membership forms and volunteer application forms.

3. All personal records will be kept under lock and key, and access limited to the Chief Officer and any authorised person only.

4. The Chief Officer, staff and volunteers will be provided with appropriate training regarding confidentiality.

5. Every member has the right to say what information should be regarded as "sensitive" and this decision is to be respected. In the event that a member has difficulty in making such a decision all information supplied, other than the basic facts required to ensure their proper care, shall be regarded a "sensitive" and shall remain confidential.

6. All members have the right to have their privacy respected. No member shall ever be pressed to give information about themselves or about their lives, past or present against their will.

7. Those members seeking help or support from staff should only be asked for sufficient information to allow the required help or support to be provided.

8. Whilst the concerns of carers will always be regarded as important, information given in confidence to the Chief Officer, staff or a volunteer should not be disclosed to a carer without permission.

9. All staff and volunteers will be asked to agree to abide by the confidentiality policy.

10. Any member who believes that confidentiality has been broken has the right to make a complaint to the Chief Officer, or to the Management Committee of El Cerezo.

11. All complaints about breaches of confidentiality will be regarded as a serious disciplinary matter and any person found to have broken confidentiality may be asked to leave.

12. El Cerezo Center will abide by the current Data Protection Act.

Exceptions
Information may only be disclosed without permission of the person concerned if:
- Disclosure is required by law eg. Police investigation of theft or suspicious death or where disclosure is essential in the course of dealing with a complaint or case of grievance or discipline.
- In circumstances of series abuse or where there is a strong likelihood harm will come to that person (including self-harm) or other matters of similar significance.

- A person is felt to lack the mental capacity to make a decision. In such a case 'implied consent' may be used to take action in the person's best interest. Such an incident must be recorded and reported.

In such cases, you must only disclose the information to your line manager or chief officer who will decide what action to take.

The minimum amount of disclosure possible will be expected in any such situation by anyone involved.

Passed by the Board of Trustees.
Signed.....
Date.....

20.- Informed Consent Form for REPLAY Project Participants

Spanish version. (1.Versión padres/ tutores)

Título del proyecto: Replay – Plataforma de juegos interactiva para la Prevención y Reintegración de los jóvenes

Declaración explicativa.

Replay pretende explorar el potencial de la simulación tecnológica de los juegos para crear espacios de colaboración que sirvan para ayudar en el proceso de rehabilitación de los niños y jóvenes que presentan un comportamiento antisocial. También como soporte en el proceso educativo de los niños y jóvenes con riesgo de presentar estos comportamientos en el futuro. El objetivo es proveer a los profesionales de una herramienta que les ayude a establecer una relación más estrecha entre terapeuta y usuario y así entender mejor las motivaciones y emociones de los jóvenes con problemas de comportamiento y con riesgo de tenerlo.

Parte I

Acepto que mi hijo participe en el proyecto de Investigación Replay. El proyecto me ha sido explicado y he leído la declaración explicativa, que puedo conservar en mi poder para el futuro. Considero que la aceptación de participación significa dar el consentimiento para que mi hijo:

- sea entrevistado por los investigadores
- utilice la plataforma de juego tecnológica
- participe en las sesiones de juego durante el periodo de testado de la plataforma
- permitir a los investigadores la medición de variables relacionados con el uso del juego de mi hijo durante las sesiones recreativas
- permitir a los investigadores el acceso a los datos referentes a las sesiones de juego de mi hijo
- que mi hijo complete cuestionarios sobre su experiencia y opinión sobre la plataforma de juego para contribuir con sus ideas al futuro desarrollo y mejora del mismo.

Protección de datos

Esta información será acumulada en un documento de seguridad que será tratado de acuerdo con la Ley de Protección de datos de mi país y que respetará los protocolos mínimos de seguridad incluidos en el D3.1, que están a disposición de los participantes en la investigación. La información personal será almacenada de forma segura durante el tiempo de duración del proyecto y tanto los datos electrónicos como aquellos en papel serán destruidos al final del mismo. Solo datos consolidados sin identificadores personales serán conservados.

La información será acumulada y procesada para el siguiente uso:

- Evaluar la capacidad del sistema para generar información significativa que contribuya a la evaluación de las sesiones de juego de mi hijo por parte de terapeutas y profesores.

Entiendo que toda la información que pueda aportar será confidencial y no podrá llevar a la identificación de mi hijo en ninguno de los informes generados por el proyecto o terceros. Ninguna información personal será publicada. La información identificable no será compartida con ninguna otra organización.

Y

Que podré tener acceso a los datos personales de mi hijo siempre que así lo requiera.

Acepto que el Centro El Cerezo almacene y procese la información de mi hijo. Entiendo que esta información será utilizada sólo para los fines especificados en este consentimiento informado y mi consentimiento está condicionado a que esta organización cumpla con las obligaciones y deberes exigidos por la Ley de Protección de datos.

Abandono del estudio.

Entiendo que la participación de mi hijo es voluntaria, que puedo elegir no participar en parte del proyecto y que puedo abandonar el estudio sin ser penalizado de ningún modo.

Nombre: .....(imprimir)
Firma: .....Fecha: .....

Parte II

Consiento el registro audiovisual de las sesiones de juego de mi hijo y su uso para publicación e investigación.

Y

Consiento la toma de fotografías de partes de las sesiones de juego de mi hijo y su uso para publicación e investigación.

Nombre: .....(imprimir)
Firma: .....Fecha: .....

Spanish version. (1.Versión expertos)

Título del proyecto: Replay – Plataforma de juegos interactiva para la Prevención y Reintegración de los jóvenes

Declaración explicativa.

Replay pretende explorar el potencial de la simulación tecnológica del juego para crear espacios de colaboración que puedan ser usados para ayudar en la rehabilitación de los niños y jóvenes que presentan un comportamiento antisocial, y como soporte en el proceso educativo de los niños y jóvenes con riesgo de presentar estos comportamientos en el futuro. El objetivo es proveer a los profesionales de una herramienta que les ayude a establecer una relación más estrecha entre terapeuta y usuario y así entender mejor las motivaciones y emociones de los jóvenes con problemas de comportamiento y con riesgo de tenerlo.

Parte I

Acepto participar en el proyecto de Investigación Replay. El proyecto me ha sido explicado y he leído la declaración explicativa, que puedo conservar en mi poder para el futuro. Considero que la aceptación de participación significa dar el consentimiento para participar en el proyecto para:

- ser entrevistado por los investigadores
- utilizar la plataforma de juego tecnológica
- participar en las sesiones de juego de los niños y jóvenes durante el periodo e testado de la plataforma
- completar cuestionarios sobre mi experiencia como experto y opinión sobre la plataforma de juego para contribuir con mis ideas al futuro desarrollo y mejora del mismo.

Protección de datos

Esta información será acumulada en un documento de seguridad que será tratado de acuerdo con la Ley de Protección de datos de mi país y que respetará los protocolos mínimos de seguridad incluidos en el D3.1, que están a disposición de los participantes en la investigación. La información personal será almacenada de forma segura durante el tiempo de duración del proyecto y tanto los datos electrónicos como aquellos en papel serán destruidos al final del mismo. Solo datos consolidados sin identificadores personales serán conservados.

La información será acumulada y procesada para el siguiente uso:

- Evaluar la capacidad del sistema para generar información significativa que contribuya a la evaluación de las sesiones de juego de los niños y jóvenes.

Entiendo que toda la información que pueda aportar será confidencial y no podrá llevar ninguna identificación en ninguno de los informes generados por el proyecto o terceros. Ninguna información personal será publicada. La información identificable no será compartida con ninguna otra organización.

Y

Que podré tener acceso a los datos personales siempre que así lo requiera.

Acepto que el Centro El Cerezo almacene y procese la información. Entiendo que esta información será utilizada sólo para los fines especificados en este consentimiento informado y mi consentimiento está condicionado a que esta organización cumpla con las obligaciones y deberes exigidos por la Ley de Protección de datos.

Abandono del estudio.

Entiendo que mi participación es voluntaria, que puedo elegir no participar en parte del proyecto y que puedo abandonar el estudio sin ser penalizado de ningún modo.

Nombre: .....(imprimir)
Firma: .....Fecha: .....

Parte II

Consiento el registro audiovisual de las sesiones de Replay del juego con los niños y jóvenes y su uso para publicación e investigación.

Y

Consiento la toma de fotografías de partes de las sesiones del juego y su uso para publicación e investigación.

Nombre: .....(imprimir)
Firma: .....Fecha: .....

English version. (1. Parents/ tutors' version)

Project title: Replay – Interactive gaming platform for Prevention and Reintegration of youths

Explanatory statement.

Replay intends to explore the potential of games' technological simulation to create areas for collaboration that serve to help in the process of rehabilitating children and youths that show antisocial behaviour. It is also intended as support for the educational process of children and youths at risk of having this behaviour in future. The aim is to provide professionals with a tool that helps them establish a closer relationship between the therapist and the user, and thereby better understand the motivations and emotions of the youths with behavioural problems and at risk of having them.

Part 1

I agree to my child participating in the Replay Research project. The project has been explained to me and I have read the explanatory declaration, which I may keep in my possession for the future. I consider that acceptance of participation means giving consent:

- for my child to be interviewed by the researchers
- for my child to use the gaming technology platform
- for my child to participate in the gaming sessions during the platform testing period
- to allow the researchers to measure variables related to my child's use of the game during the recreational sessions
- to allow the researchers to access information referring to my child's gaming sessions
- for my child to fill in questionnaires about his/her experience and opinion about the gaming platform in order to contribute with his/her ideas to the future development and improvement of it.

Data protection

This information will be collected in a security document that will be treated in keeping with the Data Protection Law in my country and shall be respected by the minimum security protocols included in D3.1, which are available to those participating in the research. Personal information shall be stored safely for the time that the project lasts, and both the electronic data and the data on paper shall be destroyed when this is over. Only consolidated data with no personal identifiers shall be conserved.

The information will be collected and processed for the following use:

- To assess the system's capacity for generating significant information that contributes to the assessment of my child's gaming sessions by therapists and teachers.

I understand that all the information that may be provided will be confidential and may not lead to the identification of my child in any of the reports arising from the project or third parties. No personal information shall be published. Identifiable information shall not be shared with any other organisation.

And

That I may have access to my child's personal data whenever I require it.

I agree to the Woolwich Polytechnic School storing and processing my child's information. I understand that this information will be used only for the purposes specified in this informed consent, and that my consent is on the condition that this organisation meets the obligations and duties demanded by the Data Protection Law.

Leaving the study.

I understand that my child's participation is voluntary, that I may choose not to participate in part of the project and I may leave the study without being penalised in any way.

Name: .....(print)
Signature: .....Date: .....

Part II

I consent to audiovisual recording of my child's gaming sessions and its use for publication and research.

And

I consent to photographs being taken of parts of my child's gaming sessions and their use for publication and research.

Name: .....(print)
Signature: .....Date: .....

English version. (1. Experts' version)

Project title: Replay – Interactive gaming platform for Prevention and Reintegration of youths

Explanatory statement.

Replay intends to explore the potential of games' technological simulation to create areas for collaboration that may be used to help in rehabilitating children and youths that show antisocial behaviour, and as support in the educational process of children and youths at risk of having such behaviour in future. The aim is to provide professionals with a tool that helps them establish a closer relationship between the therapist and the user, and thereby better understand the motivations and emotions of the youths with behavioural problems and at risk of having them.

Part I

I agree to participate in the Replay Research project. The project has been explained to me and I have read the explanatory declaration, which I may keep in my possession for the future. I consider that acceptance of participation means giving consent to participate in the project in order to:

- be interviewed by the researchers
- use the gaming technology platform
- participate in the gaming sessions of the children and youths during the platform testing period
- fill in questionnaires about my experience as an expert and opinion about the gaming platform

so as to contribute with my ideas to the future development and improvement of it.

Data protection

This information will be collected in a security document that will be treated in keeping with the Data Protection Law in my country and shall be respected by the minimum security protocols included in D3.1, which are available to those participating in the research. Personal information shall be stored safely for the time that the project lasts, and both the electronic data and the data on paper shall be destroyed when this is over. Only consolidated data with no personal identifiers shall be conserved.

The information will be collected and processed for the following use:

- To assess the system's capacity for generating significant information that contributes to the assessment of the children's and youths' gaming sessions.

I understand that all the information that may be provided will be confidential and may not lead to any identification in any of the reports created by the project or third parties. No personal information shall be published. Identifiable information shall not be shared with any other organisation.

And

That I may have access to the personal data whenever I require it.

I agree to the Woolwich Polytechnic School storing and processing the information. I understand that this information will be used only for the purposes specified in this informed consent, and that my consent is on the condition that this organisation meets the obligations and duties demanded by the Data Protection Law.

Leaving the study.

I understand that my participation is voluntary, that I may choose not to participate in part of the project and may leave the study without being penalised in any way.

Name: .....(print)
Signature: .....Date: .....

Part II

I consent to audiovisual recording of the Replay gaming sessions with the children and youths and its use for publication and research.

And

I consent to photographs being taken of parts of the gaming sessions and their use for publication and research.

Name: .....(print)
Signature: .....Date: .....

Versiunea in limba romana. (1. Parents/ tutors' version)

Titlul proiectului – Platforma interactiva de jocuri pentru prevenirea si integrarea tinerilor

Nota explicativa

Replay are ca scop explorarea potentialului simularii tehnologice a jocurilor in crearea cailor de comunicare destinate facilitarii procesului de reabilitare a copiilor si tinerilor cu manifestari antisociale. De asemenea, se doreste un sprijin in educatia copiilor si tinerilor expusi unor astfel de comportamente in viitor. Scopul este de a furniza profesionistilor mijloacele necesare stabilirii unei relatii mai stranse intre terapeut si utilizator, prin aceasta imbunatatind intelegerea motivatiilor si sentimentelor tinerilor cu tulburari de comportament sau predispusi la a le avea.

Partea intai

Sunt de acord ca fiul/fiica meu/mea sa faca parte din echipa de cercetare Replay. Proiectul mi-a fost descris si am citit nota explicativa, pe care o pot pastra si pe viitor. Consider ca acceptul pentru participare presupune ca sunt de acord ca fiul /fiica mea sa:

- fie intervievat de cercetatori
- foloseasca platforma tehnologica de joc
- participe in sesiunile de jocuri din timpul testarii platformei
- fie masurate variabilele utlizarii jocului de catre copil de catre cercetatori
- in timpul sesiunilor de recreere sa procure informatii echipei de cercetare cu privire la sesiunile de joc
- sa completeze chestionare cu privire la experienta si parerile lui/ei despre platforma de jocuri pentru a contibui cu idei la dezvoltarea si imbunatatirea ulterioara a acesteia.

Securitatea informatiei

Informatiile vor fi stocate intr-un document securizat conform normelor Legii Securitatii informatiei din tara mea si vor respecta protocoalele de minima securitate incluse in D3.1, legi puse la dispozitie participantilor la cercetare. Datele personale vor fi stocate intr-un loc sigur pe durata desfasurarii proiectului, urmand ca informatiile pe suport electronic, cat si cele pe hartie sa fie distruse in momentul incheierii acestuia. Vor fi pastrate numai datele finale lipsite de continut personal.

Informatia va fi adunata si procesata in urmatoarele scopuri:

- identificarea capacitatii sistemului pentru a genera informatii semnificative care contribuie la evaluarea sesiunilor de joc ale fiului/fiicei mele de catre terapeuti si profesori.

Inteleg ca toate datele furnizate sunt confidentiale si nu presupun identificarea copilului meu in vreunul din rapoartele inerente proiectului sau ale vreunui tert. Nicio informatie personala nu va fi facuta publica. Informatia identificabila nu va fi transmisa nici unei alte organizatii.

Si

Liber acces la datele personale ale copilului meu.

Sunt de acord cu stocarea si procesarea datelor privitoare la copilul meu de catre *Rotalent.* Inteleg ca aceste date vor fi folosite exclusiv pentru scopurile specificate in aceasta declaratie de consintamant, si ca acceptul meu se bazeaza pe conditia ca organizatia sa intruneasca regulile si indatoririle prevazute de Legea Protejarii Informatiei.

Retragerea din proiect

Inteleg ca participarea copilului meu este voluntara si ca am dreptul sa nu particip in toate sectiunile proiectului si ca ma pot retrage fara a fi penalizat in vreun fel.

Nume: .....(print)
Semnatura: .....Data: .....

Partea a doua
Sunt de acord cu inregistrarea unui material audio-vizual a sesiunilor de joc ale copilului meu si cu folosirea acestuia spre publicare si cercetare.

Si

Sunt de acord cu luarea de fotografii pe durata sesiunilor de joc.

Nume: .....(print)
Semnatura: .....Data: .....

Versiunea in limba romana (1. Varianta expertilor)

Titlul proiectului – Platforma interactiva de jocuri pentru prevenirea si integrarea tinerilor
Nota explicativa

Replay are ca scop explorarea potentialului simularii tehnologice a jocurilor in crearea cailor de comunicare destinate facilitarii procesului de reabilitare a copiilor si tinerilor cu manifestari antisociale. De asemenea, se doreste un sprijin in educatia copiilor si tinerilor expusi unor astfel de comportamente in viitor. Scopul este de a furniza profesionistilor mijloacele necesare stabilirii unei relatii mai stranse intre terapeut si utilizator, prin aceasta imbunatatind intelegerea motivatiilor si sentimentelor tinerilor cu tulburari de comportament sau predispusi la a le avea.

Partea I
Sunt de acord sa particip in proiectul Replay. Proiectul mi-a fost descris si am citit nota explicativa, pe care o pot pastra si pe viitor. Consider ca acceptul pentru participare presupune ca sunt de acord ca:

- sa fiu intervievat de cercetatori
- sa folosesc platforma tehnologica de jocuri
- sa particip la sesiunile de joc ale copiilor si tinerilor pe perioada de testare a platformei
- sa completez chestionare cu privire la experienta mea ca expert si parerile personale despre platforma de jocuri pentru a contribui cu idei la dezvoltarea si imbunatatirea ulterioara a acesteia.

Securitatea informatiei

Informatiile vor fi stocate intr-un document securizat conform normelor Legii Securitatii informatiei din tara mea si vor respecta protocoalele de minima securitate incluse in D3.1, legi puse la dispozitie participantilor la cercetare. Datele personale vor fi stocate intr-un loc sigur pe durata desfasurarii proiectului, urmand ca informatiile pe suport electronic, cat si cele pe hartie sa fie distruse in momentul incheierii acestuia. Vor fi pastrate numai datele finale lipsite de continut personal.

Informatia va fi adunata si procesata in urmatoarele scopuri:

- identificarea capacitatii sistemului pentru a genera informatii semnificative care contribuie la evaluarea sesiunilor de joc ale fiului/fiicei mele de catre terapeuti si profesori.

Inteleg ca toate datele furnizate sunt confidentiale si nu presupun identificarea copilului meu in vreunul din rapoartele inerente proiectului sau ale vreunui tert. Nicio informatie personala nu va fi facuta publica. Informatia identificabila nu va fi transmisa nici unei alte organizatii.

Si

Liber acces la datele mele personale

Sunt de acord cu stocarea si procesarea datelor mele de catre *Rotalent.* Inteleg ca aceste date vor fi folosite exclusiv pentru scopurile specificate in aceasta declaratie de consintamant, si ca acceptul meu se bazeaza pe conditia ca organizatia sa intruneasca regulile si indatoririle prevazute de Legea Protejarii Informatiei.

Retragerea din proiect

Inteleg ca participarea mea este voluntara, ca am dreptul sa nu particip in toate sectiunile proiectului si ca ma pot retrage fara a fi penalizat in vreun fel.

Nume: .....(print)
Semnatura: .....Data: .....

Partea a doua
Sunt de acord cu inregistrarea unui material audio-vizual a sesiunilor de joc in care sunt implicat si cu folosirea acestuia spre publicare si cercetare.

Si

Sunt de acord cu luarea de fotografii pe durata sesiunilor de joc.

Nume: .....(print)
Semnatura: .....Data: .....

20- Explanatory Statement

1. Executive summary

During W1 and W2, experts from the three participating countries (England, Romania and Spain) defined and selected the exercises which in their judgement may help to better identify the onset of antisocial behaviour, to be included in the REPLAY gaming platform.

These exercises are common in the ASB prevention programmes, and through the AIJU they have been turned into games.

The experts in ASB have defined and agreed on the activities that we should include in Replay to make this platform a point of reference as a tool for professionals in social re-education. The requirements have also been specified that should be taken into account in developing the prototype from a technological point of view in order for it to be suited to the end users.

With all of the prior work, the first version of the Replay platform's functional Prototype has been created. Over the coming months it will be tested in its real context of use in order to identify strengths and weaknesses that will enable the product to be made as similar as possible to what its target users expect of it.

2. Introduction

The main aim of this short document is to clarify and inform accurately about the method that is to be used in the impact study of the Replay gaming platform's first prototype.

As defined in the DoW, the validation of this prototype within the impact study will include:

- **Firstly,** a study on the prototype's **ergonomics**, both for its primary users (children) and its secondary users (experts and professionals).
- **Secondly**, we will study the Replay **platform's playability** in terms of **motivation** for the users while playing the game and the possible difficulties that may arise during the testing procedure, also for the two types of user.
- **Thirdly**, we will analyse the **preventative and educational worth** that the experts attribute to the platform in its use as a tool by social therapists and professionals.

3 Methodological triangulation

In order to gather all the information that we need in our impact study and be able to make a suitable analysis of all the variables, we will use a methodology designed ad hoc that is based on a "mixed" or "triangulated" methodology.

Both quantitative and qualitative analyses will be used in this methodology in order to get a complete view of the real situation studied, and we will involve these methods in a single study to be able to analyse the consistency of the findings by means of different methods.

4 Sample (1)

Children from 10 to 14 years of age of both sexes and with a low level of antisocial behaviour as the target of the REPLAY platform. The following chart gives details of the sample according to age and sex:

	PRIMARY USERS				TOTAL
	BOYS		GIRLS		
	10-12 YEARS	12-14 YEARS	10-12 YEARS	12-14 YEARS	
PRIMARY SCHOOL	30	-	30	-	60
SECONDARY SCHOOL	-	30	-	30	60
TOTAL	30	30	30	30	120

	SECONDARY USERS		TOTAL
	EXPERTS	TEACHERS	
	Psychologists, Occupational Therapists, social workers....	Primary and secondary school teachers	
TOTAL	18	18	36

4 Sample (2)

Moreover, 36 secondary users, 12 from each country, will participate in the testing sessions, giving their specialised opinions and suggestions on the process for improving the tool.

The coordinating staff for the centres in Spain, Romania and the UK will actively participate in the gaming sessions. These coordinators will be trained to teach the users how to operate the tool and to ensure that the necessary information is collected during the testing process.

Thus, each session will involve the participation of:
1 primary user (boy or girl from the sample)
1 secondary user (an expert or teacher)
1 coordinator from the centre

To carry out the sessions, the necessary security protocols for research with children will be taken into account, which will be applied in all the testing centres and with all the users. To do so, we will use the International ICC/Esomar code for social and market research[1] as our basis.

[1] ICC/Esomar code; available from:http://www.esomar.org/index.php/codes-guidelines.html

5 The Timing of the Testing

The first version of the prototype with all of the educational and entertainment activities operational will be implemented in September in the three testing centres:

Romania – Rotalent
Spain – El Cerezo
UK – Woolwich Polytechnic School.

For 40 working days, the platforms for testing will be available so that at least the data from a minimum of 160 hours of use of the platform by the users and experts will be available.

In each centre, an informative training session will be held prior to the gaming sessions to train the experts and teachers in how the platform works and in the method for testing, questionnaires, specific aims, etc. Here, the informed consent sheets will be given to the participants who decide to remain in the study, and those who do not wish to continue with the experience will be removed from the sample.

6.1.Criteria for the ergonomic evaluation

Methods for the ergonomic evaluation

To evaluate the platform's ergonomics, it is important to use different methods that enable all the ergonomic problems presented by the product to be compared and analysed. To begin this part of the impact study, all the general ergonomic requisites will be summarised for games and specifically for this target age group.

3 methods will be used:

- ***Heuristic evaluation with checklist*** (with **secondary users**: experts and teachers).
- ***Cognitive walkthrough*** (with **primary and secondary users**)
- ***Breakdown analysis*** (with **primary users**)

6.2 Criteria for verification of the level of Playability

For the platform to be successful in the future, it is important to know the user's subjective point of view, and as well as verifying how the Replay tool functions it is essential to make an in-depth study of the assessments made by the primary and secondary users. In this part of the study we shall verify if the platform's design is in line with the primary and secondary users' expectations as regards playability. It is essential to show that the platform, involving educational activities, is evaluated with high levels of motivation.

This is why we study the **levels of motivation** that the tool generates. To this end, questionnaires will be issued at the end of the sessions. Some time afterwards, a **Focus Group** will also be held.

This study on the levels of acceptance must be dealt with both for primary users (children) and secondary users (experts and teachers).

The Flow Theory perspective will be at the centre of the motivational studies. This is understood to be "The state in which people are so involved in an activity that nothing else seems to matter; the experience itself is so enjoyable that people will do it for the sheer sake of doing it" (Csikzentmihalyi, 1990 and Voelkl, 2003).

6.3. Criteria for the study on the assessment of Replay as a tool for professional development.

It is important to emphasise that playing video games frees one from certain prejudices that are difficult to express in real life. Replay may serve as an aid to express real situations or emotions in the young ones' lives and thereby prevent situations of antisocial behaviour when these are at their lowest levels.

One fundamental feature of the REPLAY tool is considered to be the fact that it boosts the **capacity for communicating** with the therapist or professional since, as is specified in the different deliverables, the originality of this tool rests on the use of the gaming session to produce feedback with a therapist or teacher upon visualising the game process carried out for a second time. If this happens, we will have met the ASB experts' basic expectation with the platform, since achieving communication with the child was one of the difficulties of the classic programmes used in ASB prevention and re-education.

For this reason, lastly, in the Post-Session a **questionnaire** will be issued to **assess the value of professional performance of the tool** (experts and teachers), a made to measure questionnaire with items that will allow their satisfaction levels and usefulness of the tool to be measured.

Summary table of the assessment instruments in Replay

	Children	Experts/teachers/ coordinators
Phase 0: **Pre-session**		**Training Session**
	Questionaire A-D: Antisocial behaviour- criminal, N. Seisdedos Cubero (1987) in the adaptation by Allsop and Feldman's scale of antisocial behaviour (1978)	- **Adaptatión** of **CBCL** (Achenbach, T. M's Child Behavior Check List ,1991)
Phase 1: **Play session**	-**Cognitive walkthrough** - **Breakdown analysis with video-analysis**	- **Heuristic** evaluation check list - **Cognitive walkthrough**
Phase 2: **"Re-play" session**		-**"Re-play" observation guide**
Phase 3: **Post-session**	- Motivation questionnaire, **Flow**/Likert scales	- Motivation questionnaire, **Flow**/Likert scales
		Questionnaire on Evaluation of the tool's professional **performance value** **FOCUS GROUP Guide**

Project coordinador:
Brainstorm
Partners from:
- AIJU
- Innovatec
- University AI.I.Cuza
- Rotalent
- Centro de día "El Cerezo"

Funded by the European Commission: