Legal aspects and evaluation of business and Cloud scenarios

Document Identification	
Date	30/10/2015
Status	Final
Version	1.0

Related SP / WP	SP 5/WP 55	**Document Reference**	D52.5
Related Deliverable(s)	52.1-4, 22.6	**Dissemination Level**	PU
Lead Participant	ULD	**Lead Author**	Rasmus Robrahn (ULD)
Contributors	Hannah Obersteller (ULD), Rasmus Robrahn (ULD)	**Reviewers**	NRS, ECS

Abstract: In this deliverable a description of the legal obstacles that came up during the legal support of the pilot system is given. In the annex, a consent form and data processing contract that were drafted for the pilot can be found.

This document is issued within the frame and for the purpose of the *FutureID* project. This project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement no. 318424.

1. Executive Summary

This deliverable provides a summary of the legal support that was provided for the pilot of work package 52. The work package aimed at demonstrating the viability of FutureID components in business scenarios. To achieve this viability, the pilot had to be developed in a way that is compliant with current legislation, especially data protection legislation.

At first an introduction to the pilot will be given. Atos runs an e-Learning platform and added the possibility to log in or register to this platform by using FutureID instead of a username/password system. Afterwards the legal obstacles will be discussed. As no other legal ground was applicable, the main legal obstacle was the validity of the consent in the context of employment. This is difficult to achieve because consent needs to be given freely, which is rarely the case in an employment context. This part of the analysis is based on an early version of the pilot. Then it will be described what changes were made to the pilot near the end of the project and how that could affect the conclusions reached for the earlier versions. It has to be noted, that it was not planned to test the pilots using any real personal data. However in preparation for real world testing, a data processing contract and consent form were drafted, which can be found in the annex to this deliverable.

2. Document Information

2.1 Contributors

Name	Partner
Hannah Obersteller	ULD
Rasmus Robrahn	ULD

2.2 History

Version	Date	Author	Changes
0.1		Hannah Obersteller	Outline
0.2		Rasmus Robrahn	First draft
0.3		Hannah Obersteller	Review for General Meeting in Stuttgart
0.4		Rasmus Robrahn	Adjustments after the General Meeting in Stuttgart
0.5		Rasmus Robrahn	Added abstract, executive summary and conclusion
0.6		Hannah Obersteller/Rasmus Robrahn	Added data processing contract and consent form
1.0	30.10.2015	Rasmus Robrahn	Included feedback from reviewers

2.3 Referenced Documents

Article 29 Working Party, WP 187, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

Article 29 Working Party, WP 48, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

Article 29 Working Party, WP 217, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Schroers/Marnau/Schlehahn/van Alsenoy

Schroers, J., Marnau, N., Schlehahn, E., van Alsenoy, B., „FutureID D22.6 Legal Requirements“ EU FP7 Project FutureID, 2013, http://futureid.eu/data/deliverables/year1/Public/FutureID_D22.6_WP22_v1.0_LegalRequirements.pdf

3. Table of Contents

4. Project Description

The *FutureID* project builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe, which integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims.

The *FutureID* infrastructure will provide great benefits to all stakeholders involved in the eID value chain. Users will benefit from the availability of a ubiquitously usable open source eID client that is capable of running on arbitrary desktop PCs, tablets and modern smart phones. *FutureID* will allow application and service providers to easily integrate their existing services with the *FutureID* infrastructure, providing them with the benefits from the strong security offered by eIDs without requiring them to make substantial investments.

This will enable service providers to offer this technology to users as an alternative to username/password based systems, providing them with a choice for a more trustworthy, usable and innovative technology. For existing and emerging trust service providers and card issuers *FutureID* will provide an integrative framework, which eases using their authentication and signature related products across Europe and beyond.

To demonstrate the applicability of the developed technologies and the feasibility of the overall approach *FutureID* will develop two pilot applications and is open for additional application services who want to use the innovative *FutureID* technology

Future ID is a three-year duration project funded by the European Commission Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318424

5. Legal Support

The task 52.6, legal support of the Atos Service Marketplace platform, aimed at assisting the partners by identifying and resolving potential legal issues from the application scenarios. The following text will provide a short explanation of the pilot and three legal obstacles that are special to the pilot system. The general legal requirements of the FutureID infrastructure are explained in the FutureID Deliverable 22.6. Although Spanish law is applicable and has been used for the contract and consent form, the discussion here will cite the provisions of the European Data Protection Directive, as the Directive sets the minimum standard in Europe and is easily accessible for international readers. The first part of this analysis is based on the presentation of the pilot at the evaluation meeting in Berlin on the 16th of June 2015. As this Deliverable had to be finished in time at the end of the project there will only be a short description and analysis of the pilot as it was presented at the last general meeting in Stuttgart on the 29th of September. It has to be noted, that the ongoing development of the pilot can change the outcome of the legal analysis and especially the legality of the data processing. It is part of the nature of legal support as a continuous work, that legal questions that arise during the development of a pilot can be analysed and discussed in a deliverable but no definite answer to the question whether a final version of the pilot is legally compliant in all possible regards can be given.

It was not planned to test the pilot with any real data as part of the FutureID project. However the analysis and legal support was aimed at preparing the pilot for real world testing. Therefore, the following discussion will assume that personal data will be processed.

5.1 E-Learning Platform

Atos runs an e-Learning platform for its employees, who can currently authenticate to the platform with a username/password-system. The platform provides the employees with online courses on internal security measures, language and product courses etc. Participation in, or successful completion of the online courses is not mandatory but may be proposed to the employees of Atos by their supervisors. Within the FutureID project an additional authentication method is implemented: authentication with FutureID. Therefore, an additional button is added to the user interface of the e-Learning platform.

The idea is to open the e-Learning platform to non-employees of Atos Spain, who do not have an employee username/password-account and therefore need other means to authenticate. However, this will not happen as part of the pilot.

Users need a smart card reader and a Spanish eID card. When clicking the “Log-in with FutureID” button, users are redirected to the Broker Service website hosted by the processor. On this website the possibility to authenticate via STORK, by using their Spanish eID card is

shown to them. If the users choose this means of authentication, they are connected to the website of STORK where the actual authentication process takes place.

5.2 Legal Obstacles

There are two main legal obstacles that are special to the e-Learning platform pilot. The first is the unnecessity of the data processing and the second is the problem of consent in an employer-employee relationship. The first problem addresses the legal principles of data minimisation and the necessity principle, while the second is related to the requirement that consent must be freely given.

5.2.1 Unnecessary Data Processing

The e-Learning platform can currently only be accessed by Atos employees using a username/password authentication method. The FutureID pilot adds the possibility of using the Spanish national eID for authentication.

Because of the principle of prohibition with permission provision in data protection law, for data processing there needs to be a legal ground, which can be a provision of the law or the legally valid consent of the data subject.[1]

Possible legal provisions are described in Article 7 (b) to (f) of the Data Protection Directive.

Member States shall provide that personal data may be processed only if:

[…]

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

[1] FutureID Deliverable 22.6, p. 29.

All of the possible legal grounds have the necessity principle in common. The necessity principle pays respect to the fact that privacy and informational self-determination are not absolute rights. In specific cases the interests of the data controller can outweigh the interests of the data subject, even if no consent is obtained. However, a strict interpretation of these provisions is necessary because it allows data processing against or without the will of the data subject.

Data processing is not automatically necessary, when it is covered by a contract.[2] It is only necessary if the contract cannot be fulfilled without the data processing.

Using the FutureID pilot to access the e-Learning platform is clearly unnecessary when keeping in mind the aforementioned requirements. This is shown by the fact that so far Atos employees were securely able to authenticate by using a username/password system which generally establishes enough trust for the purposes of an e-Learning platform. Even if one would argue that data processing in the context of the e-Learning platform is generally necessary for the performance of the labour contract there is no necessity for the use of the FutureID pilot and the processing of associated data like the STORK Identifier. The contract could still be fulfilled by using a username/password system. The necessity principle does not take into account that an authentication through FutureID might be more secure. In principle, the pilot creates a new data processing workflow and includes a new entity (Spanish STORK peps) without purpose.

5.2.2 Consent of Employees

As there is no legal provision for data processing applicable to the pilot, Atos has to obtain legally valid consent from its employees. According to Art. 2 (h) of the Data Protection Directive consent

"shall mean any freely given specific and informed indication of [the data subjects] wishes by which the data subject signifies his agreement to personal data relating to him being processed."

Consent can be a weak – or even invalid – justification for the processing of personal data if its limits are not clearly outlined. One of those limits is the requirement that the consent must be given freely, which means that the data subject must have an actual choice. There may not be a risk of deception, intimidation, coercion or significant negative consequences if the data subject does not consent.

Especially in cases where the data subject is under the influence of, or dependent on the data controller, it can be doubted whether consent was given freely, because the data subject might

[2] Article 29 Working Party, WP 217, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 16.

worry that she will be treated worse in the future if she does not fulfil the wishes of the data processor.[3]

One of those cases is the relationship between employer and employee. The employee might be able to refuse consent but fears the consequences of doing so. The Article 29 Working Party stated that "where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 as it is not freely given. If it is not possible for the worker to refuse it is not consent."[4]

However, if there are sufficient guarantees that the consent is really free, it can even be used in situations of subordination.[5]

For the e-Learning platform it can be argued that consent is possible although it is obtained in a subordination relationship. As there is still the possibility of using the username/password authentication method employees have a real choice if they want to use the FutureID pilot or the already established system. Even if they chose not to consent they would still have access to the e-Learning platform. On the other hand it can still be argued that an employee might feel pressured to consent because he worries that it could have negative effects on the employer-employee relationship if he does not help his employer test a new authentication system. This shows how problematic consent in the employment context is, even if denying consent factually does not have negative effects, which is also very hard to determine and depends significantly on the corporate culture and the way the employees are approached.

For the FutureID pilot the use of consent as a justification for data processing is possible but only if Atos Spain makes sure, that their employees do not feel pressured to consent.

5.2.3 Relevancy of the Data

According to the relevancy principle of Art 6 (1) (c) of the Data Protection Directive only such data shall be processed that is

adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed.

Whether the pilot is in compliance with the relevancy principle is questionable because the STORK Identifier is processed.

---

[3] Article 29 Working Party, WP 187, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, p. 13.
[4] Article 29 Working Party, WP 48, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, p. 23.
[5] Article 29 Working Party, WP 187, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, p. 14.

First, the purpose of the data processing has to be determined. Two different purposes seem possible. If the purpose is the authentication to the e-Learning platform, then the STORK Identifier is not relevant as authentication can be done with a username/password-system. However, if the purpose is to authenticate at the e-Learning platform through the FutureID pilot, then the STORK Identifier is relevant as it is needed for the functioning of STORK.

The purpose here is defined by the consent of the employees. The consent (see Annex) was drafted for the conduction of the pilot within the FutureID project. In the consent form it is explicitly stated that the employees consent to the authenticating by using the FutureID client. Therefore the purpose cannot be limited to authentication at the e-Learning platform but must be defined as authentication through the FutureID pilot.

5.3 Ongoing Development of the Pilot

After the evaluation workshop in Berlin on the 15th and 16th of June the pilot was further developed. At the general meeting in Stuttgart on the 29th of September, Atos showed a version of the pilot that only asks the user for the eIdentifier. This identifier is now a hashed version of the STORK Identifier. When a user wants to authenticate to the e-Learning platform by using FutureID the Broker Service gets the STORK identifier, surname, name and more from the STORK PEPS. The STORK identifier is then hashed and only the hashed version of the identifier is sent to the e-Learning platform. The hash operation is different for each service provider, which reduces linkability significantly, because it increases the difficulty for different service provider to collude with each other.

Additionally, Atos planned to support not just the Spanish National eID but also the Fraunhofer Card, a test version of the German eID (nPA), the Belgian eID and software certificates. This change is supposed to show how FutureID could be used to authenticate users from different countries and companies.

A short legal analysis came to the conclusion that still no other legal ground than consent can justify the data processing.

Article 7 (b) of the Data Protection Directive is still not applicable. If Atos and, e.g., Fraunhofer enter into a contract where the employees can get access to the e-Learning platform by authenticating through FutureID, the data processing that happens when a user logs in or authenticates could be viewed as necessary for the performance of this contract. However, Article 7 (b) of the Data Protection Directive is only applicable if the data subject is party to the contract, which wouldn't be the case. There are other possible contractual solutions to this problem but they would be very specific to each state and its labour and contract laws. A possible solution could be a contractual framework provided by Atos and Fraunhofer, which would lead to individual contracts between Atos and the employees of Fraunhofer, which could then justify data processing based on Article 7 (b) of the Data Protection Directive.

For the purpose of developing and testing a pilot, which is the scope of this deliverable and the legal support, it would be sufficient to obtain informed and freely given consent from each employee that participates in the pilot.

6. Conclusion

As was shown, in the case of testing the integration of FutureID into the Atos e-Learning platform, consent can be a valid justification for the data processing. In the special case of this pilot it is justified to allow for valid consent in the employment context, but this cannot be generalised as in most other cases the consent will not be given freely.

Other legal grounds are not applicable. For the future development of the pilot it is absolutely necessary that the developing entities make sure that all changes are still in compliance with the applicable legislation.

7. Annex: Documents

During the project runtime it turned out that the e-Learning platform pilot would not use real employees' personal data but the application would be tested using dummy data. Nevertheless, a consent form, a processing contract and a privacy policy were drafted, under the assumption that the pilot would have been tested with the participation of real users' personal data. As these documents were drafted for an early version of the pilot, they would need to be changed if they were to be used for testing with real personal data.

7.1 Annex I: Processing Contract

Contract between ATOS and ECS on the processing of personal data pursuant to Art. 12 of the Spanish Data Protection Act 1999 (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal) and the provisions of the Royal Decree 1720/2007 of 21 December which approves the regulation implementing organic law 15/1999, of 13 December, on the protection of personal data (Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal)

Agreement

between

Atos SA– Calle de Albarracin, 28037 Madrid, Spain, as the data controller in the sense of Art. 3 (d) Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (hereinafter Spanish Data Protection Act)

hereinafter: Controller

and

ECSEC GmbH, Sudetenstrasse 16, 96247 Michelau, Germany, as the data processor in the sense of Art. 5 (i) of the Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (hereinafter Royal Decree 1720/2007)

hereinafter: Processor

Preamble

This agreement specifies the data protection obligations of the parties which arise from the realisation of the eLearning pilot of the project "FutureID – Shaping the future of electronic internet" (FutureID). The FutureID project receives funding from the European Community's Seventh Framework Programme (Call: FP7-ICT-2011-8) under Grant Agreement n° 318424. This data processing agreement solely addresses the question of processing personal data in the course of the realisation of the eLearning pilot as practically implemented in the FutureID project. Furthermore, this data processing agreement solely addresses the relationship between Controller and Processor for the subject matter. It does not affect any legal relations between the parties established in the Grant Agreement, nor any rights and duties set forth in the FutureID consortium agreement, specifically any rights and duties related to intellectual property remain untouched. The Processor runs the FutureID component "Broker Service" and provides the Controller with an additional way of authentication for users of the eLearning platform run by the Controller. This contract is just regulating the legal relation between Controller and Processor. It does not affect further parties involved in the authentication process.

Subject Matter and Duration

The subject-matter of this agreement is the collection and processing of personal data for the realisation of the FutureID e-Learning platform (e-Learning pilot) as implemented during the project runtime. The Processor provides the Controller with set-up, administration, debugging, controlling the performance and maintenance of the running system concerning the FutureID component "Broker Service", which serves as an intermediary between the Controller and the Spanish National STORK PEPS.

For allowing the employees and external users of the Controller (users) to authenticate with FutureID to the e-Learning platform, a data exchange between the Atos network and the FutureID Broker Service, run by the Processor, is necessary. If a user chooses to authenticate via FutureID, the personal data needed for this operation (name, surname, STORK identifier) is transmitted from the user to the Processor. The data's origin is the Spanish national eID. In order to verify the data he receives, the Processor will transmit the data to the Spanish National STORK PEPS. After the Spanish National STORK PEPS has carried out the verification process, the data is transmitted to the Processor who will pass the data on to the Controller. The Controller stores the verified data and grants access to his e-Learning platform for the user. For the fulfilment of the aforementioned tasks of the Processor it is not necessary to access the Controller's systems.

The processing on behalf of the Controller ends with the termination of the FutureID project. Correlating, the rights and obligations of this agreement's parties are valid during the project runtime. Any personal data of the pilot participants shall be deleted once they are no longer needed to fulfil the duties resulting from this agreement - at the latest, six months after the end of the project, unless legislation imposed on this agreement's parties requires the retention of specific data. In that case, the Processor warrants that he will guarantee the confidentiality of this data and that he will not actively process this data anymore.

Overview and Explanation of the e-Learning Pilot in FutureID

The data processing takes place as part of the e-Learning pilot. In the following, we will provide a quick overview and explanation. The information is also provided to the participating data subjects in the sense of Art. 5 Spanish Data Protection Act on the information of data subjects as part of the consent form (annex II).

The Controller runs an e-Learning platform for his employees, who can currently authenticate to the platform with a username/password-system. The platform provides the employees with online courses on internal security measures, languages, products and similar topics. Participation in, or successful completion of none of the online courses is mandatory but may be proposed to the Controller's employees by their supervisors. Within the FutureID project an additional authentication method is implemented: authentication with FutureID. Therefore, a further button is added to the user interface of the e-Learning platform.

The idea is to open the e-Learning platform to non-employees of Atos Spain, who do not have an employee username/password-account and therefore need another means to authenticate.

Users need a smart card reader and a Spanish eID card. When clicking the "Log-in with FutureID" button, users are redirected to the Broker Service website hosted by the processor. On this website the possibility to authenticate via STORK, by using their Spanish eID card is shown to them. If the users choose this authentication means, they are connected to the website of STORK where the actual authentication process takes place.

Nature of the personal data involved

The following categories of personal data related to the participating data subjects will be collected and processed and are thus subject-matter of this agreement:

- Personal master data: surname(s), first name(s)
- STORK identifier

Persons affected

The data subjects affected by the processing of aforementioned personal data are the voluntary participants in this pilot, who can namely be:

- Employees of the Controller

All of the data subjects participating have been handed out information about the project and the pilot itself.

Employees of the Controller have been asked to provide explicit consent to the processing of their aforementioned personal data. The data subjects have been informed that the participation is free and voluntary as authentication to and use of the Atos e-Learning platform will still be possible by username/password-authentication. The data subjects have also been informed that they may revoke their consent and withdraw from the pilot at any time (cf. documents in annex 2).

As far as third parties will use the pilot application, the Controller will provide them with the same information material and obtain their consent by using the consent form (annex 1) before they may access the e-Learning platform.

Overview of the Pilot Setup and Data Processing

The Controller is providing his employees with the infrastructure including hardware and software to use the e-Learning platform. This includes the operation of the system, i.e. the operation and maintenance of the machines the platform is run on.

For authentication with FutureID, the user presses the "Authenticate with FutureID" button located at the starting web page of the e-Learning platform.

For allowing the employees of the Controller and external users (hereinafter: users) to authenticate with FutureID to the e-Learning platform, a data exchange between the Atos network and the FutureID Broker Service, run by the Processor, is necessary.

If a user chooses to authenticate with FutureID, the personal data needed for this operation (name, surname, STORK identifier) is transmitted from the user directly to the Processor. The Processor's task is to provide the Controller with the personal data of the user he needs to have verified to allow users to enter his e-Learning platform. Therefore, the Processor will obtain a verification of the data from the STORK system and provide the Controller with the information he receives: The user's data's origin is the Spanish national eID. In order to verify the data he received, the Processor will transmit the data to the Spanish National STORK PEPS. After verification by the Spanish National STORK PEPS the data is transmitted to the Processor who will only then pass the data on to the Controller. The Controller stores the verified data and grants access to his e-Learning platform for the user.

After having authenticated themselves with username/password or with FutureID, the system allows the employees to participate in certain online courses.

In summary, the Controller fulfils the following tasks:

- Providing his employees with the necessary hardware to use the system (card readers, workplace with desktop PC or notebook, servers, firewalls, routers)
- Providing the necessary software to use the system (User software, web applications)
- Maintaining the system,
- Issuance and administration of employee accounts,
- Debugging/troubleshooting, and controlling the performance and maintenance of the system overall,
- Providing and keeping up to date course content.

The Processor is administering the Broker Service system running on machines which reside on the premises of the Processor's sub-contractor [PLEASE FILL IN]. Contractual relations between the Processor and [SUB-CONTRACTOR] are not touched by this agreement. In case the Processor intends to migrate the Broker Service system to another machine – albeit a machine located on his own premises – he will inform the Controller in advance.

The Processor provides authentication with FutureID as described above.

The Processor supports the Controller with the set-up, administration, debugging, controlling of performance and maintenance of the e-Learning platform as far as it concerns the integration of the authentication method "authentication with FutureID". In doing so, the Processor is fully subjected to the instructions of the Controller.

In the general overview of the pilot, the Broker Service is an autonomous entity.

In order to integrate the authentication method "authenticate with FutureID", the Controller will give the Processor access to the e-Learning platform.

[At this point a detailed definition of the data flows would have to be provided. Such definition was not available at the time of the drafting]

Obligations of the Controller

The Controller agrees and warrants:

The Controller ensures that the processing of personal data in the FutureID e-Learning pilot has been and will be conducted in accordance with the relevant provisions of the applicable provisions of the Spanish Data Protection Act and the Royal Decree Royal Decree 1720/2007.

The Controller has instructed and throughout the duration of the FutureID e-Learning pilot will continue to instruct the Processor how to process the pilot participant's personal data on behalf of the Controller and in accordance with the applicable Spanish Data Protection Law, especially Article 20 of the Royal Decree 1720/2007 and Article 12 of the Spanish Data Protection Act.

The Controller ensures that sufficient guarantees are given with respect to the necessary technical and organisational measures to protect the personal data of the pilot participants in accordance with Article 9 of the Spanish Data Protection Act. Thereby, the specific measures which will be conducted by the Processor on behalf of the Controller (as described above) are taken under instruction and supervision of the Controller. Art. 88 Royal Decree – the security document and its requirements

The Controller will collect voluntary and informed consent from the participating data subjects prior to the processing of their personal data within the pilot pursuant to Article 11(1) of the Spanish Data Protection Act, Art. 10 Royal Decree 1720/2007. While doing so, the Controller will inform the concerned data subjects about the means and purpose of the personal data processing. Moreover, the Controller agrees to make a copy of this agreement available to the data subjects upon request.

Obligations of the Processor

Typically, the Processor only gets access to data which is non-personal. But for technical tasks stemming from this agreement (e.g. error troubleshooting) it cannot be ruled out that it might become necessary to grant access to files which contain personal data. The following obligations only apply in this exceptional case. Therefore, the Processor agrees and warrants:

The Processor ensures that personal data processed on behalf of the Controller are processed strictly in compliance with the controller's instructions set out in this agreement and as given throughout the pilot. The processing of the personal data is limited to the purpose of the pilot, namely the authentication to the Atos eLearning platform with FutureID.

The Controller oversees the actions of the Processor within the eLearning pilot. The Processor is obliged to provide the Controller with all necessary information which the Controller may not able to retrieve herself. This especially concerns data breach notifications and other issues which need problem resolve.

In the exceptional case that the Processor gets access to files still containing personal data, he is obliged to take appropriate technical and organisational measures to protect the personal data of the pilot participants in accordance with Article 9 of the Spanish Data Protection Act and Title VIII of the Royal Decree 1720/2007. These measures are defined in the following section.

Technical and organisational measures

In this section, the necessary technical and organizational measures pursuant to Article 9 of the Spanish Data Protection Act and Title VIII of the Royal Decree 1720/2007, as to be implemented by the Processor under instruction of the Controller, are defined.

The Processor must document that necessary technical and organisational measures stipulated in this section are taken before starting to process the data, thereby giving details of the actual process to be followed, and must present this to the Controller for review. When accepted by the Controller, the documented measures will form the basis of the processing. If something raises the need for amendments, these must be applied amicably.

The technical and organizational measures are subject to technical progress and development, and the Processor may implement adequate alternative measures. These must not however fall short of the level of security provided by the specified measures. Any material changes must be documented.

The necessary measures are defined in the following subsections.

Access Control

The Processor has to prevent that unauthorized entities gain access to data processing systems for processing or using personal data. Systems with personal data falling under this agreement need to be stored in a secure place such as offices of the Processors premises in Michelau, Germany, locked away or be kept under personal control of an authorized person.

Employees of the Processor that need access to these systems can only do so with a smart card and pin.

The Processor prevents that data processing systems are being used without authorization. For this the computers used by the Processor are personalized to one user and use a strong encryption. Access rights to files containing personal data falling under this agreement will be limited to personnel working on the FutureID project.

The Processor ensures that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. In the case of log files ... If the Processor gets non-anonymised files, those should be deleted once the particular information is not needed anymore for the subject matter (e. g. after completed debugging task).

Confidentiality

The Processor ensures that all personal data received or collected in the context of the FutureID e-Learning pilot remains confidential, meaning it cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Moreover, it must be possible to ascertain and check which entities are authorized to receive personal data using data transmission facilities. Data storage mediums will be fully encrypted. The Processor must not transmit any personal data falling under this agreement to other entities than the Controller.

The controller is aware that the data transfer is not end-to-end encrypted.

Input control

The processor relies on the data he receives from the STORK PEPS. He ensures that it is possible to check and ascertain whether personal data have been entered into, altered or removed from data processing systems after the fact and if so, by whom.

Availability

The Processor helps to ensure that personal data are protected against accidental destruction or loss.

He will not store data persistently, except for logs. These log files will only contain the IP-Addresses and will be kept for a week.

The necessary availability of the administration support is not governed by this agreement.

Data separation

The Processor ensures that data collected for different purposes can be processed separately. The Processor does not merge any personal data with own or third persons data. Data processed on behalf of other Controllers or for other purposes must be stored and treated separately.

Trusted Data Processing Device

The Processor ensures that the device being used to receive and to process the data sent by the Controller can be trusted. The processing device must therefore be regularly updated with security patches of his operating system. On top of that, regular security scans of his data processing device must be triggered by state-of-the-art anti-virus software.

Additionally he will protect his systems with a regularly updated firewall and intrusion detection systems.

Right to rectification, erasure and blocking of data

The Processor may only correct, delete or block the data processed on behalf of the Controller when instructed to do so by the Controller. If a user should directly ask the Processor the correction or deletion of his personal data, the Processor forwards this request to the Controller without delay.

Breach notification

In case the personal data under control of the Processor within the eLearning platform System is subject to accidental or unauthorized access, process, or disclosure, the Processor must inform the Controller concerning the incident by notice without delay after discovery. This notice shall contain as far as the Processor is able to identify:

- The nature of the incident,
- The type of data accessed, processed, or disclosed,
- The cause of the incident, or
- Who made the unauthorized use/who received the unauthorized disclosure,
- If and which countermeasures have been taken
- If and which preventive actions shall be taken to mitigate deleterious effects of the incident

The Processor shall provide this information and eventual additional information, as reasonably requested by the Controller, as written report.

Enforcement of data subject's rights

The concerned data subjects whose personal data is being processed within the FutureID eLearning pilot have rights, which may be exercised towards the Controller according to Articles 13 to 19 of the Spanish Data Protection Act and Article 23 to 36 of the Royal Decree 1720/2007, which include e. g. rectification, deletion, blocking of data. The Processor may only rectify, delete or block the data processed on behalf of the Controller when instructed to do so by the Controller. If a user should directly ask the Processor for the correction or deletion of his personal data, the Processor is obliged to forward this request to the Controller without delay.

Sub-contracts

Without prior written permission of the Controller the Processor is not allowed to let sub-contractors process personal data falling under this agreement.

[At this point fill in sub-contractors, such as external server providers]

Cooperation with supervisory authorities

The Controller agrees to deposit a copy of this contract to the responsible data protection supervisory authority if it so requests, or if such deposit is required under the Spanish Data Protection Law.

The parties of this contract agree that the supervisory authority has the right to conduct an audit of the eLearning platform if it so requests.

Further provisions

The following subsections are a restatement of the German Data Protection Law (Datenschutzgesetz, BDSG) under which is applicable to any processing of personal data by the Processor residing in Munich, Germany,

- The Processor has a data protection officer appointed, § 4f BDSG.
- The Processor must choose the persons that carry out the data processing with respect to their professional qualifications and personal integrity. Such persons shall be obligated when taking up their duties to maintain confidentiality, § 5 BDSG.
- The Processor maintains a documentation with the information stipulated in § 4e BDSG, § 4g (2) BDSG.
- As for the applicable national data protection law the following is assumed: As the Controller is located in Madrid, Spain, the processing of personal data and the requirements regarding this contract is governed by Spanish Data protection law. The processing of any personal data once transferred to the processor is governed by this contract, instructions given the by the Controller and the German Data Protection Act (BDSG) directly applicable to the Processor.

On behalf

Atos (Controller)

Madrid, ___ MONTH 2015

_____

ECS (Processor)

Michelau, ___ MONTH 2015

_____

7.2 Annex II: Consent Form

Information Sheet

Dear Atos employee,

Atos now offers a second way to sign in or register on the ATOS e-Learning platform. In addition to using your username and password you can now also use the FutureID Client through the provided FutureID button on the authentication screen. This allows you to authenticate yourself by using the Spanish national eID (DNIe).

What is FutureID?

FutureID is an EU-funded research and development project. It aims to extend the reach of eIDs to new market sectors and population segments while providing an easy to use client that supports multiple platforms.

The FutureID infrastructure will provide great benefits to all stakeholders involved in the eID value chain. Users will benefit from the availability of a ubiquitously usable open source eID client that is capable of running on arbitrary desktop PCs, tablets and modern smart phones. FutureID will allow application and service providers to easily integrate their existing services with the FutureID infrastructure, providing them with the benefits from the strong security offered by eIDs without requiring them to make substantial investments. This will enable service providers to offer this technology to users as an alternative to username/password based systems, providing them with a choice for a more trustworthy, usable and innovative technology.

Currently the users can authenticate to the Atos e-Learning platform with a username/password system. The platform provides the employees with online courses on internal security measures, languages, products. Participation in or successful completion of none of the online courses is mandatory but may be proposed to the Atos employees by their supervisors. Within the FutureID project an additional authentication method is implemented: authentication with FutureID. Therefore, a further button is added to the user interface of the e-Learning platform.

And STORK?

STORK is a platform that allows people to use their national eID in foreign countries by connecting the national eID infrastructures.

[At this point a detailed explanation of the functioning of STORK would have to be provided]

How to authenticate to the Atos e-Learning platform with FutureID

For authentication with FutureID, the user presses the “Authenticate with FutureID” button located at the starting web page of the e-Learning platform.

For allowing the employees of Atos and external users (hereinafter: users) to authenticate with FutureID to the e-Learning platform, a data exchange between the Atos network and the FutureID Broker Service, run by ECSEC GmbH, is necessary.

If a user chooses to authenticate with FutureID, the personal data needed for this operation (name, surname, STORK identifier) is transmitted from the user directly to ECSEC. It is ECSEC's task to provide Atos with the personal data of the user they need to have verified to allow users to enter their e-Learning platform. Therefore, ECSEC will obtain a verification of the data from the STORK system and provide Atos with the information they receive: The user's data's origin is the Spanish national eID. In order to verify the data they received, ECSEC will transmit the data to the Spanish National STORK PEPS. The STORK PEPS is a national gateway that acts as an intermediary for foreign eIDs towards its domestic Service Providers. After verification by the Spanish National STORK PEPS the data is transmitted to ECSEC who will only then pass the data on to Atos. Atos stores the verified data and grants access to their e-Learning platform for the user.

After having authenticated themselves with username/password or the FutureID button, the system allows the employees to access the internal area of the Atos e-Learning platform.

The following Data will be processed by Atos, ECSEC and STORK for identification and authentication purposes:

- STORK Identifier
- First Name
- Last Name

The STORK Identifier is a unique, session based number which is provided by the STORK infrastructure.

Your rights

You have the right to request and obtain free of charge information on your personal data subjected to processing, on the origin of such data and on their communication or intended communication.

You have the right to rectify or cancel the processing of data whose processing is not in accordance with the provisions of the Law 15/1999 of 13 December on the Protection of Personal Data or when the data is incomplete or incorrect.

How is my data kept secure?

[PLEASE FILL IN]

Questions?

If you have any questions regarding the information provided to you, please don't hesitate to contact Atos.

Contact details:

Atos SA– Calle de Albarracin, 28037 Madrid, Spain

ECSEC GmbH, Sudetenstrasse 16, 96247 Michelau, Germany

Consent Form

This consent form addresses you as a participant in a pilot of the FutureID authentication system within the EU-funded research and development project FutureID. The pilot will be integrateted into the Atos e-Learning system and will allow the users to authenticate themselves by using a Spanish national eID (DNIe). During this trial, the participant's personal data will be collected, stored and processed by the Atos e-Learning platform and processed by ECSEC. For this, Atos kindly asks you for your consent to process the said personal data. For an explanation of FutureID and the type of personal data processed for which purposes, please refer to the information sheet handed out as attachment to this form. Further information about the technical specifics can be found under the project website (www.futureid.eu).

The following personal information will be processed when using FutureID for authentication on the Atos e-Learning platform:

- STORK identifier
- First Name
- Last Name

Beyond this personal data used to authenticate you on the Atos e-Learning platform other personal data may find its way into the system through the content uploaded by the users to the e-Learning platform.

You have the right to withdraw your consent at any time without providing a reason by notice towards Atos. Not providing consent or revoking it later will not cause any disadvantages when using the Atos e-Learning platform. Without giving consent you will not be able to authenticate or register to the Atos e-Learning platform with your eID. You will still be able to authenticate or register by using your username and password.

By signing this form you declare that you have read and understood the information provided to you in this consent form and in the information sheet.

You also declare that you hereby explicitly consent to voluntarily participate in the trial under the above described terms.

The explicit expression of consent includes the later usage of the collected and processed personal data in aggregated (i. e. anonymised) form for scientific research aimed at improving the FutureID technology and for correlating research and dissemination publications.

Date: _____

First Name: _____

Last Name: _____

Signature: _____

Please give the signed consent form to: [Please fill in contact at Atos]

Contact information: Atos SA– Calle de Albarracin, 28037 Madrid, Spain