SEVENTH FRAMEWORK PROGRAMME

ENDORSE

Legal Technical Framework for Privacy Preserving Data Management

ENDORSE

Deliverable D2.3

Trials Scenario Specification

Editor:	Stefania Marrara, Giulia Prandi
Deliverable nature:	Report
Dissemination level: (Confidentiality)	Public
Contractual delivery date:	31/08/11
Actual delivery date:	
Suggested readers:	Consortium
Version:	00.06.00
Total number of pages:	30
Keywords:	User Scenarios, Trials

Abstract

This deliverable includes the outcomes of the analysis carried out in task 2.4 after the delivery of D2.1 Trials Scenario Preliminary Specification in February 2011. In the months since, the scenarios presented in D2.1 were further analysed and enriched to reach a complete description of what we envision, from the target user Company point of view, as the outcome of the Endorse project. The final outcome of this deliverable is a set of five macro-scenarios or clusters including scenes and situations aimed at covering all possible use situations for ENDORSE, from the privacy protected data storage and use cases to the life cycle of the PRDL rules.

Disclaimer

Neither the ENDORSE consortium as a whole, nor a certain party of the ENDORSE consortium warrant that the information contained in this document is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using this information.

Impressum

Legal Technical Framework for Privacy Preserving Data Management

ENDORSE

Workpackage: WP2 Requirements

Title: D3.2 Privacy Rule Definition Language Preliminary Specification

Editors: Giulia Prandi, EurA, Stefania Marrara, SN

Authors: Giulia Prandi, EurA, Massimo Nichetti, EurA, Stefania Marrara, SN,Thomas Kurz, SUAS, Christoph Rücker, SUAS

Workpackage leader: Ronald Leenes, TILT

Estimated number of PMs spent on preparing the deliverable: 7.0 PM

Copyright Notice

Executive summary

Task 2.4 activity inside the ENDORSE project is to provide a set of Trial Scenarios able to drive the completion of both the PRDL language and the platform, and, at the same time, provide a robust benchmark for the trials of the project. This deliverable follows and completes Deliverable 2.1 Initial Scenarios which focused on the situation which characterizes the privacy data management inside the two target companies Europ Assistance and Seecomms.

In this deliverable we present a set of scenarios useful to describe how Endorse will change the way data privacy is managed by European Companies.

There are 5 sets of scenarios divided on the basis of the main topic they cover. Another important division is due to the Company which is the environment of the scenario itself.

Scenarios were based on the practices available inside the target Companies:

- Europ Assistance, an insurance company with one product, Docticare, devoted to medical assistance
- Seecomms, a communication company whose main product is a kind of social network with many different situations in which personal data are gathered, stored or, in case, transmitted to third people.

The construction of the trial scenarios was initiated by a brainstorming which involved partners from both WP2 Requirements and WP3 Architecture aimed at evaluating the most important state of the art methodology approaches to drive the construction of the scenarios and the requirements elicitation process suitable for Endorse. The approaches reviewed are presented in Deliverable 3.1 Functional Architecture which shows in detail the full process from the scenario description to the requirements extraction and filtering.
The full process of collecting requirements was based on a 5 stage process to collect and specify both functional and technical requirements. The entire process was the result of a strict cooperation between WP2, Requirements, WP3.1, Functional Requirements and WP 3.2 Technical Architecture.

The scenarios provided in this deliverable and the output of the legal requirements task and the social requirements task in work-package 2 provides the final input for the developers of the PRDL (Privacy Rules Definition Language) and the (software) developers of the policy engine. This document provides a example-based idea of what the language should be capable of expressing and where and how the policy engine can fit into existing and future systems.

Unfortunately Seecomms, due to internal reasons, decided to leave the Endorse project at the end of May. This deliverable treasured the experience gained during the months of work with Seecomms but was edited and completed by Europ Assistance and Soluta.Net who helped the task 2.4 leader to finalise this effort. The Seecomms scenario's will not be realised in the demonstrators as such, but components and ideas will be used.

List of authors

Participant	Author
EurA	Giulia Prandi
SN	Stefania Marrara
EurA	Massimo Nichetti
Acknowledgement	
SUAS	Thomas Kurz
SUAS	Christoph Rücker
Internal Reviewer	
TILT	Ronald Leenes
UniZar	Pedro Bueso

Table of Contents

List of figures

1 Introduction

The activity of Task 2.4 of the ENDORSE project is to provide a set of Trial Scenarios able to drive the completion of both the PRDL language (Privacy Rules Definition Language) and the platform, and, at the same time, provide a robust benchmark for the trials of the project. This deliverable follows and extends the Deliverable 2.1 Initial Scenarios which focused on the situation which characterizes the privacy data management inside the two target companies Europ Assistance and Seecoms.

The main objective of this document is to

- provide examples of business processes (from the point of view of end-users) in the environments offered by Europ Assistance (hereafter EurA) and Seecoms (the trial enterprises) for running trials with the ENDORSE tools.
- give an overview of relevant use case scenarios and set out the main requirements of the trial enterprises.
- allow other partners in the ENDORSE project to base their work on real world scenarios.
- provide a realistic starting point for the ENDORSE technical developers to develop a toolset to provide monitoring, logging and filtering of the engines for data access and data handling policy (including privacy statements) compliance.
- assist in the development of an adequately generic toolset applicable beyond the trial scenarios suitable for adoption within organisations and businesses outside the ENDORSE project, in particular European SMEs.
- help, by provision of examples and scenarios, other project partners understand business operations of the trial enterprises, and factors which are likely to be taken into account in any decision whether to adopt a toolset.
- provide a set of examples of preliminary PRDL grammar in order to help the design of the PRDL language syntax and semantics with the aim to to achieve an expressive but user-friendly language.

We concentrated on 19 scenarios that we gathered into 5 main clusters based on the topic they cover.

The scenarios provided in this deliverable, together with the output of the legal requirements task and the social requirements task in work-package 2, provides the final input for the developers of the PRDL and the (software) developers of the policy engine. This document provides an example-based idea of what the language should be capable of expressing and where and how the policy engine can fit into existing and future systems.

1.1 Methodology

The construction of the trial scenarios was initiated by a brainstorming which involved partners from both WP2 Requirements and WP3 Architecture aimed at evaluating the most important state of the art methodology approaches to drive the construction of the scenarios and the requirements elicitation process suitable for ENDORSE. The approaches reviewed are presented in Deliverable 3.1 Functional Architecture which shows in detail the full process from the scenario description to the requirements extraction and filtering.

The full process of collecting requirements was based on a 5 stage process to collect and specify both functional and technical requirements. The entire process was the result of a strict cooperation between WP2, Requirements, WP3.1, Functional Requirements and WP 3.2 Technical Architecture.

The stages of the requirements elicitation process are:

1. Scenario brainstorming;
2. Gathering of initial requirements;
3. Scenario evaluation, analysis, ranking, filtering and refinement;
4. Refinement of functional and non-functional requirements and extraction of use cases;
5. Harmonisation, prioritisation and ranking of requirements.

In the process of scenario brainstorming (phase 1 of the list above), Task2.4 partners produced several stories trying to capture and extend the features mentioned in the description of work (DoW). The scenarios were created on the basis of meetings and colloquia with people from Europ Assistance and Seecomms who tried to gather their desiderata w.r.t. the system-to-be in their companies. At this stage, the focus was to identify the main stakeholders involved and to capture the behavioural aspects of the system and.

After a first feedback process from people of WP3, in the third stage of the process the initial scenarios were evaluated, prioritised, and, subsequently, compiled into new refined scenarios following the feedbacks obtained by Europ Assistance (EurA) and Seecomms. These scenarios were built so as to include multiple scenes and map all the companies desiderata features. Furthermore, the scenarios were harmonised to demonstrate the same level of detail. At the end of this stage, the refined set of scenarios was ranked, sorted and filtered. A selected set of final scenarios was eventually produced.
The final set of scenarios are the focus of this deliverable and are shown in detail in the following.
In the following we provide a detailed description only of the two phases regarding the scenarios.
The complete description of the process is available in D3.1 Functional Architecture

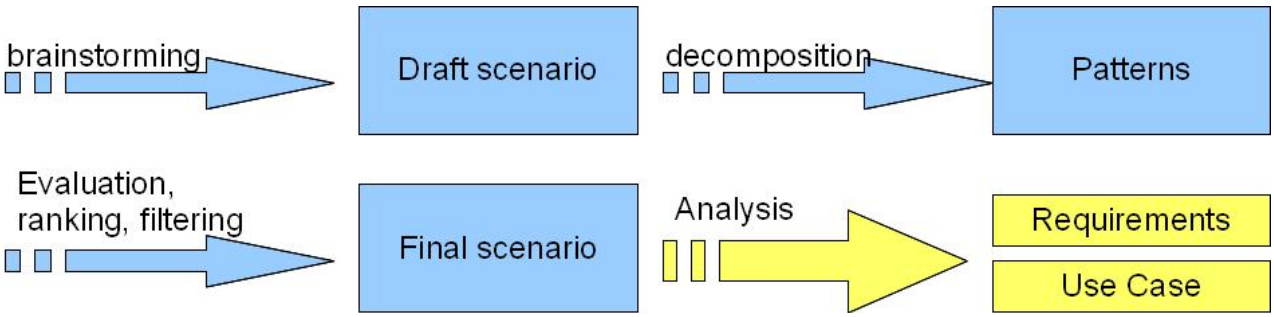

Figure 1: The scenarios and requirements elicitation process

The elicitation process is shown in Figure 1. In blue (dark pattern) the part of the process that produced the set of scenarios presented in this work, in yellow the part included into D3.1 Functional Architecture.

2 Trial Scenarios

In this chapter we detail the scenarios gathered in task 2.4 and divide them into five main topics that try to envision the use of ENDORSE system inside Europ Assistance and Seecomms

The five topic we envisioned are:

1. Rule Life Cycle Scenarios explaining how a rule is created, how and when updated or queried, and finally deleted.
2. Access Control Scenarios showing how ENDORSE will filter the access to privacy protected data
3. Data Life Cycle Scenarios describing how personal data can be gathered, maintained and deleted in a privacy compliant way.
4. Reporting on data usage scenarios describing how ENDORSE can be of help to the Data Controller in all those reporting activities required by the law (in particular the Italian law)
5. Endorse and back-end systems interactions Scenarios showing how Endorse will interact with the back end systems of the Company

2.1 Rule Life Cycle Scenarios

The scenarios presented in this section describe several situations in which rules are created, updated, deleted.

2.1.1 EURA_01_01 Creating Rules

Background: Giulia is a EurA employee responsible for data privacy policies/statements.

She wants to use the ENDORSE system for typing in some EurA rules for the Docticare platform usage[1].

Scene 1:

Giulia accesses the ENDORSE system using her user-id and password. The system shows the expected page identified by Step 1 in Figure 2.

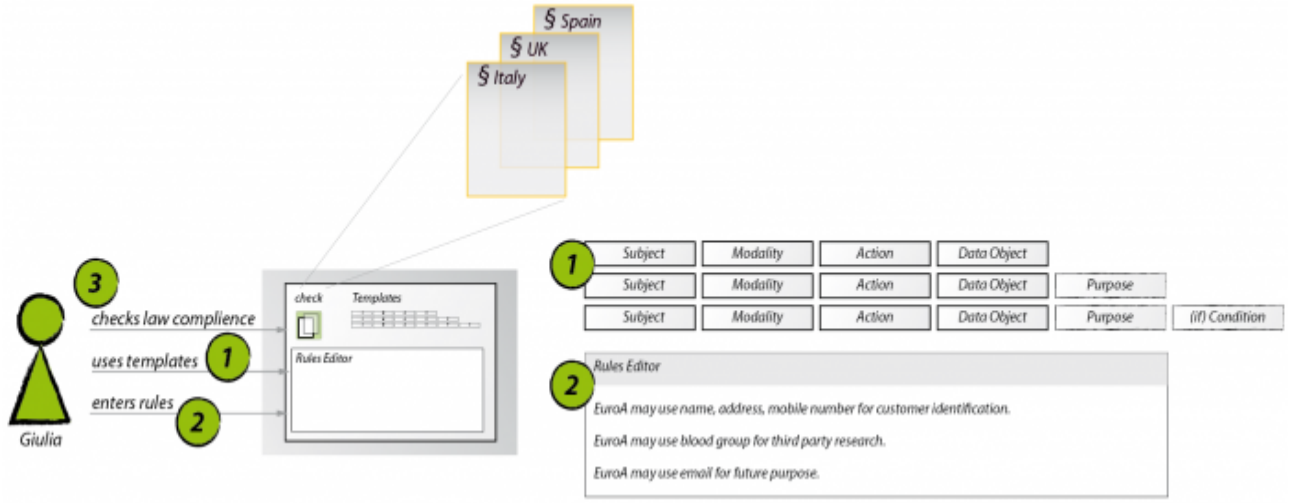

Figure 2: The system behaviour

[1] A complete description of Docticare can be found in D2.1 Trials Scenario Preliminary Specification.

The ENDORSE system provides PRDL templates (Step 1 - Figure 2) for defining rules. Giulia wants to enter the following three rules in PRDL:

1. Europ Assistance wants to use name, address, mobile number for customer identification.
2. Europ Assistance wants to use blood group for third party research.
3. Europ Assistance wants to use customers e-mail for future purposes.

Giulia can directly write in the free text window of the system or use the templates with some options for graphical drag and drop.

There are templates for expressions with purpose or without, with conditions and without (Step 1 in Figure 2). Based on the template structure and supported by some drop-downs, e.g., for the modalities (MAY, MUST, ...), Giulia defines the data privacy rules (Step 2 - Figure 2).

Scene 2:

After entering the desired set of rules, Giulia wants to check the rules for compliance with the Italian law for data privacy. She uses the check-button (Step 3 – Figures 2 and 3) and selects to check her rules with the Italian law. There is a library for some national and international laws already expressed in PRDL and Giulia just has to import them into her system. Based on a colour schema (green, yellow, red), the system provides her feedback on the on the status of the rules she entered in view of the Italian law (Step 4 – Figures 3). There might be some conflicts (red) when she tried to express rules which are conflicting with law. The feedback uses a colour schema (green, yellow, red) to depict the rule compliance with the relevant regulation. **Red:** Direct Conflict with Legislation. **Yellow:** Possible Conflict with Legislation. **Blue:** Check cannot be completed or rules cannot be validated because expressions are not known or not specific enough. **Green:** No identified conflict with Legislation.

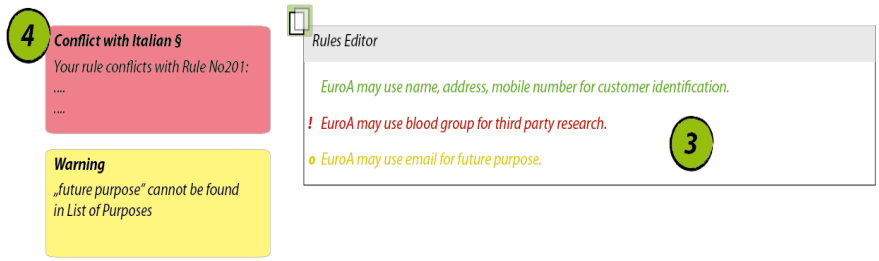

Figure 3: Rules check results

Now, Giulia can modify the rules to avoid conflicts and warnings and check them again until she is satisfied with the result.

2.1.2 EURA_01_02 Endorse as a Repository of Rules for EurA's Employees

Background: A Marketing employee has to launch an online competition to promote Docticare.

Scene 1:

Laura, a marketing department employee has to launch an online competition to promote Docticare: she has to check if there are particular rules in the EurA rule set related to online competitions.

Laura fills in an ENDORSE rules search text box with some relevant words, like: *online competition, consent for marketing purposes*... She launches the search of rules available in the rule

repository matching the keywords.

The ENDORSE system returns a list of rules related to the item.

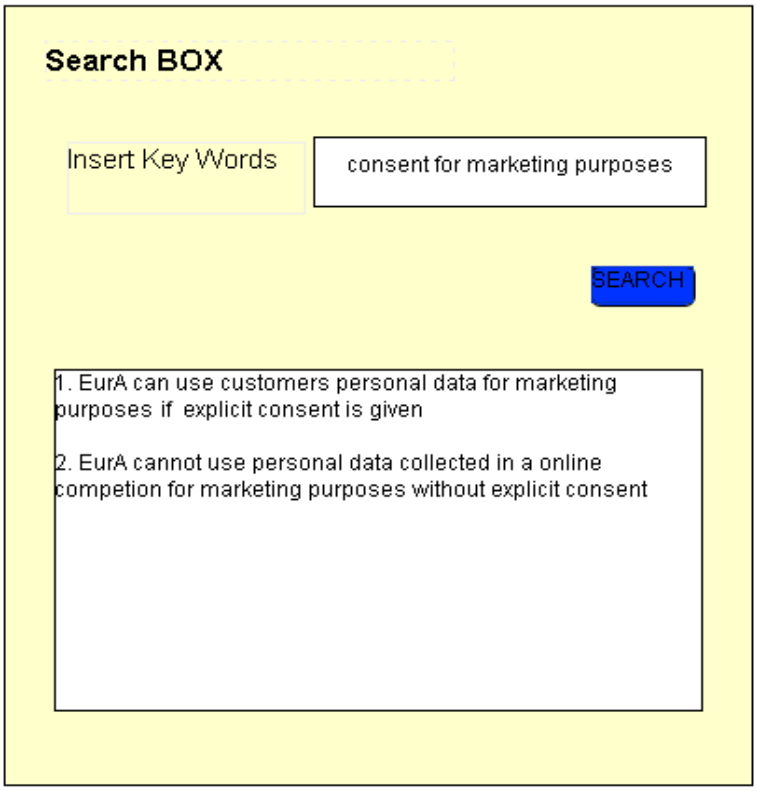

Figure 4: The keyword based search of rules

Scene 2:

Based on the search result, Laura asks to a supplier to develop a full privacy compliant website.

2.1.3 EURA_01_03 Updating and deleting rules

Background: Italian Government has just signed a new legislation about data protection. Giulia, as EurA data protection officer, has to update the rules which are affected by the new law.

Scene 1:

Giulia opens the Endorse Consortium website and downloads the new legislation PRDL library to update the EurA internal Endorse system.

Scene 2:

Giulia now wants to check if the EurA rules inside the repository are compliant with the new legislation.

Giulia selects from a menu the function “Check the compliancy”. A new windows opens which allows Giulia to select the legislation against which she wants the check and to choose between a complete EurA rules repository scan or just the check of a selection of rules.

Scene 2a:

option 1 – complete scan:

Giulia asks the ENDORSE system to scan every rules in the internal repository against the selected legislation.

The system returns a list of rules that are not compliant or whose validation was not possible using the colour code described in the Eura 01_01 scenario.

option 2b – scan of a selection:

Giulia knows that only some internal rules are potentially affected by the new legislation.

She chooses the “check selection” option which opens a new window with a list of all the internal PRDL rules. In this window Giulia can select the rules she wants to be verified.

The system returns a list of those rules that are not compliant or whose validation was not possible using the colour code described in the Eura 01_01 scenario.

Scene 3:

Giulia selects one of the rules that are marked as conflicting.

The ENDORSE system opens the editing window (see Eura 01_01 scenario) in which Giulia may change the rule and verify it again against the legislation.

In this window she is also allowed to delete a rule from the repository.

2.1.4 See_01_01 Creating Rules

Background:

The SeeComms staff responsible for data privacy policies and statements wishes to use the Endorse system to create and verify compliance of a new feature of the SeeComms system with data protection rules.

Scene 1:

When outlining the new feature, the SeeComms developers are tasked to discuss the feature with the SeeComms personal data protection official regarding the data protection impact and produce a data impact analysis. The SeeComms staff, in simple terms, map the use of the data in relation to any new feature.

Scene 2:

After logging into the ENDORSE system, the staff uses the graphical drag and drop feature to map the way the new feature works. There are templates for expressions with purpose and conditions. Based on the template structure and supported by some drop-downs, e.g. for the modalities (MAY, MUST, ...), the Privacy rule within PRDL is created.

Scene 3:

It is now necessary to check the rules with the relevant data protection laws for data privacy. The SeeComm's staff member has discussed matters with the SeeComms personal data protection official and identified the countries for which relevant data protection rules apply. (In SeeComms this utilises the two-letter geographic code used for domain names).

The SeeComms staff member then needs to check the proposed rule against the relevant laws. They opt for the "“Check the compliancy”"as shown in scenario EURA_01_03. The result provided by the system uses a colour schema (green, yellow, red) to depict the rule compliance with the relevant regulation. **Red:** Direct Conflict with Legislation. **Yellow:** Possible Conflict with Legislation. **Blue:** Check cannot be completed or rules cannot be validated because expressions are not known or not specific enough. **Green:** No identified conflict with Legislation.

Scene 4:

Yellow and Blue marked rules are passed to the personal data protection official who checks the PRDL language against the Report and the SeeComms stated privacy statement and makes necessary

adjustments. Step 3 is repeated for each relevant country after appropriate amendments to the PRDL Language.

Once the report is acceptable, the SeeComm's personal data protection official signs off the PDRL as complete.

Scene 5:

Based on the PRDL accepted rules, the users will receive audited reports of relevant data usage.

2.1.5 See_01_02 Rule system Usability

Background: John is working for SeeComms. He is responsible for the data privacy rules at SeeComms.

SeeComms staff responsible for data privacy policies and statements wish to use the Endorse system to create and verify compliance of a new feature of the SeeComms system with data protection rules.

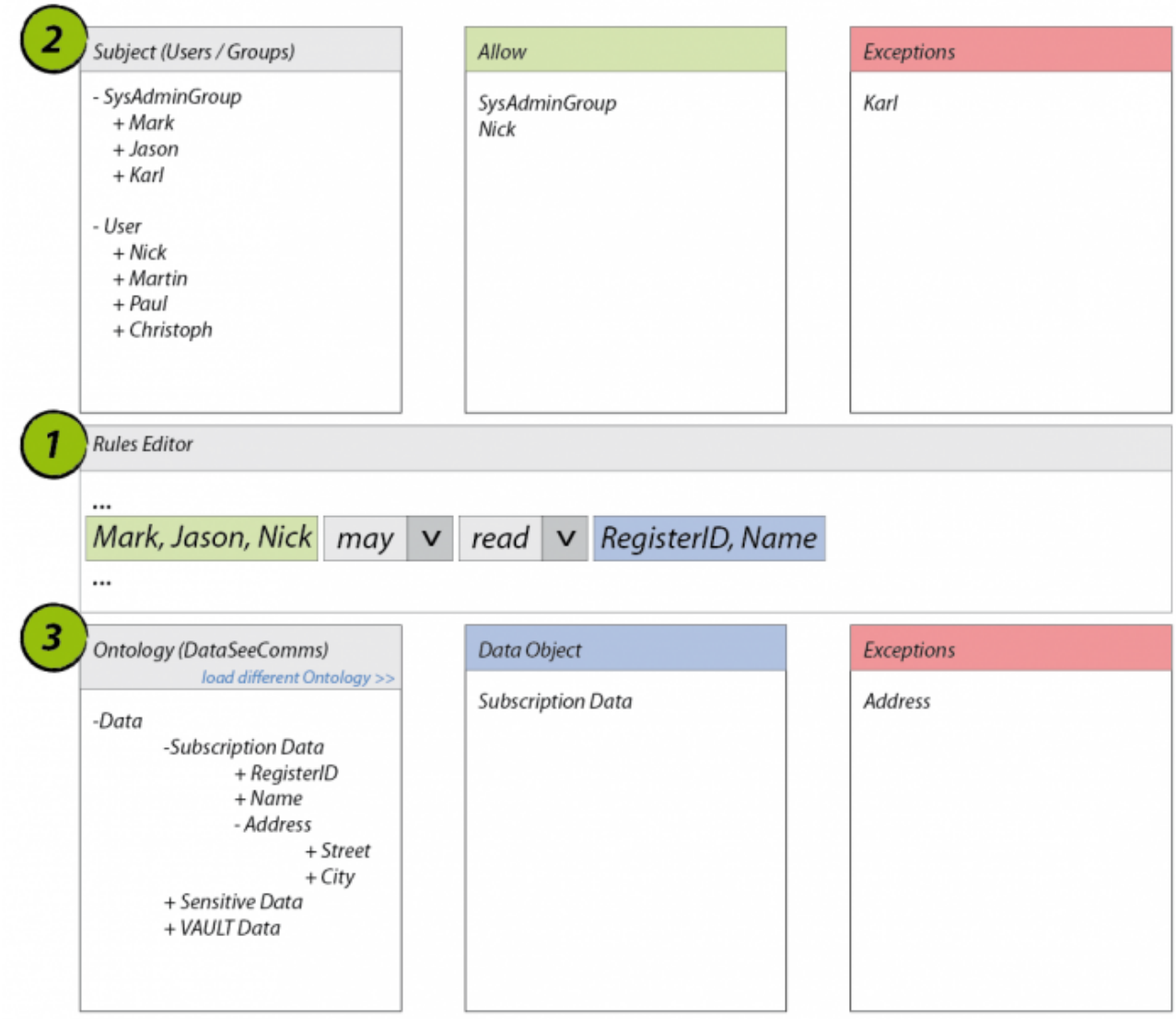

Figure 5: Access control rules with groups usage

Scene 1:

The ENDORSE system provides PRDL templates (see EURA_01 (Figure 2)) for defining rules.

John decides to choose the Subject>>Modality>>Action>>Data Object template to add a rule on data access (Step 1 in Figure 4).

Scene 2:

The ENDORSE system provides a drag and drop feature (Step 2 in Figure 4) for defining the Subject, i.e. in this case single users and groups. In order to ease the usage of the system, there are three boxes for defining the Subject: 1) "Subject (Users/Groups)", 2) "Allow" and 3) "Exceptions". When users or groups are dropped in the "Allow" and "Exception" box, the system view (Step1 in Figure 4) is updated automatically with the corresponding users/groups. If there is an exception to a group, the individual group entries are listed up individually in the rule itself.

At SeeComms there are two user groups: *SysAdminGroup* and *User*. John wants to define the rule for all members of *SysAdminGroup* and uses the drag and drop feature to add them in the "Allow" box. He decides that Karl, although a member of the SysAdminGroup, is not allowed to access the data and therefore drops his name to the "Exceptions" window. Additionally, Nick is also allowed to read the data concerned.

Scene 3:

Equivalent to SEE_02_02, the "Data Object" can also be defined by using a drag and drop feature (Step3 in Figure 4). In this scenario, SeeComms defined a DataSeeComms Ontology, which refers to the data concepts, terms and structures, used by SeeComms. John can define Data Objects and Exceptions here. The rule is again automatically adapted according to the selected "Data Objects".

2.2 Access Control Scenarios

2.2.1 EURA_02_01 Create, check and modify an authorization profile

Background

EurA as Data Controller has to configure an authorisation system for every person or for an homogeneous set of persons in charge of the processing prior to the processing itself. Moreover, every year EurA has to verify that the prerequisites for retaining the relevant authorisation profiles still apply.

Scene 1: creating a new authorisation

Linda, a new employee, enters in EurA marketing dept: Michelle, the Marketing Manager, asks for the creation of a new user account and the coupling with a specific profile.

Michelle opens the Endorse system which provides a form in which she can easily see the existing profiles for the persons in charge of the processing at the Marketing dept.

Michelle decides that the existing profiles do not match the tasks Linda has to fulfil. So she asks for the creation of a new profile for Linda.

The system provides a list of the types of processing and the related IT applications.

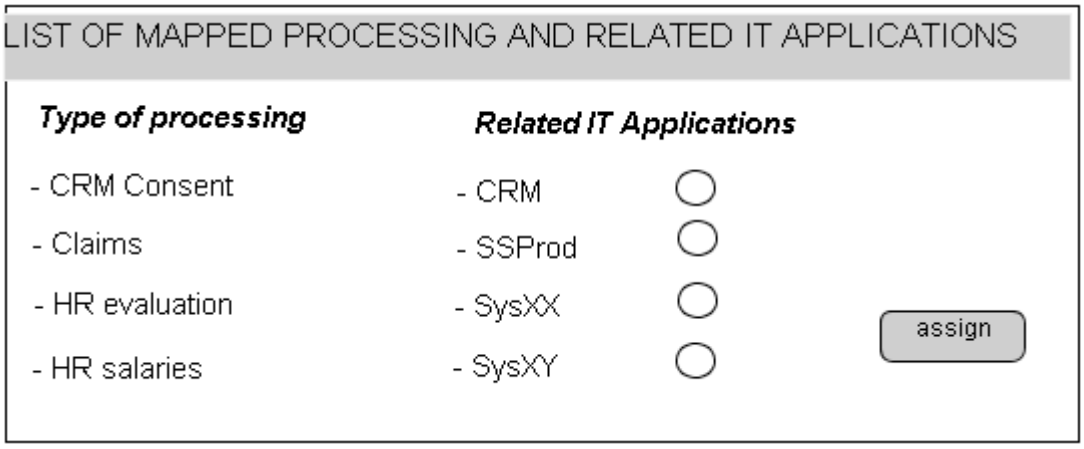

Figure 6: Systems and corresponding Data processing types

Michelle clicks on “create a new profile” and gives to it the name “marketing and communication”. She chooses from the list provided by the system the processing/applications she wants to attribute to the profile “marketing and communication” just clicking on a button "assign" (Figure 6)

The graphical interface hide the following rule editing process.

Rule: [Person_in_charge_of_the_processing] MAY [use] [applications] FOR [process_data]

The new profile “marketing and communication” has been created.

Michelle chooses this new profile and link it together the name of Linda.

Michelle upload into Endorse system the request for a new user account creation.

Endorse requires to the User mngt system the new user credentials which are then provided to Michelle.

Scene 2: querying for authorizations

Michelle has decided to give to Linda a task previously assigned to Simone.

The task is related only to the processing of “data consent on CRM”. Simone's profile is “Marketing

1".

Michelle has to check whether the profiles of the persons belonging to her area are correct, in particular the one who was attributed to Simone.

She asks to Endorse system to list the authorisation profiles of the persons in charge of the processing associated to the Marketing area. ENDORSE provides the requested list.

Michelle checks whether the authorisation to a particular processing (and so to the related IT applications) given to the profile "marketing 1" has to be maintained or has to be deleted. So she clicks on the profile "marketing 1" and all the processing and related IT applications are shown.

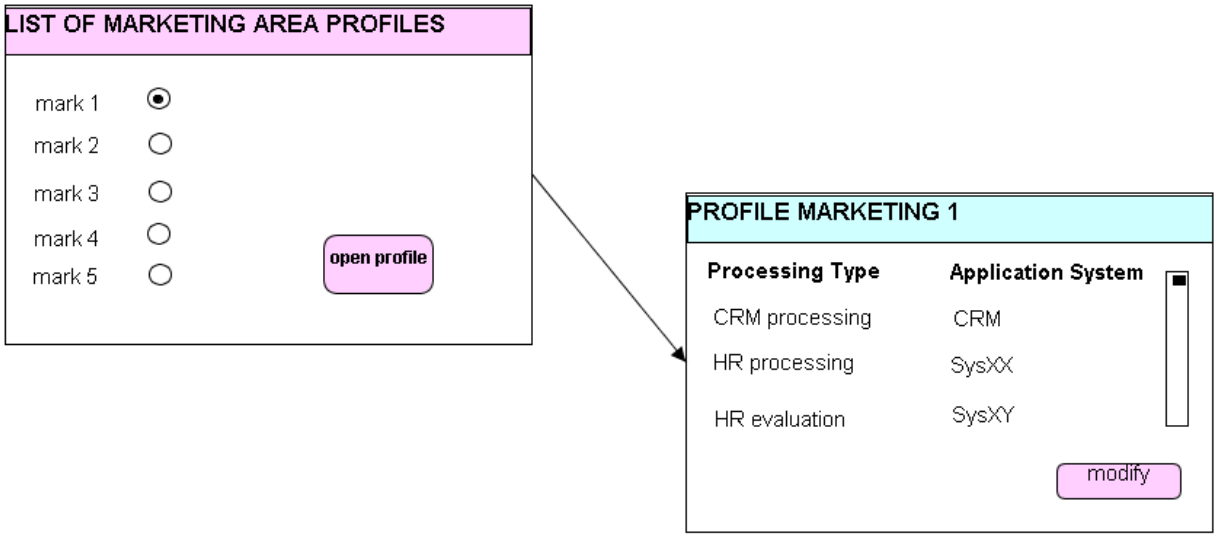

Figure 7: Managing profiles

She decides that, since Simone no longer performs the task she has now assigned to Linda, she has to delete from the profile "marketing 1", the processing called "data consent on CRM".

The rule hidden in this process preformed using the GUI is:

Rule: [Person_in_charge_of_the_processing] MAY NOT [use] [applications] FOR [process_data]

Michelle selects the processing "data consent on CRM" and push on the button delete.

Simone with her updated profile will no more access to the applications related to the process "data consent on CRM".

2.2.2 EURA_02_02 External DataAccess by DocCharly

Background: DocCharly is a doctor in Germany. Stefania holds a Docticare contract with EurA. Stefania is on vacation in Germany and consults DocCharly. DocCharly needs to access Stefania's medical files through the Docticare frontend.

Scene 1:

Stefania had an accident during her vacation in Germany and is consulting DocCharly for his

advice.

Stefania has filled her medical passport in Docticare website.

Stefania has created a token to allow a third person to read a predefined pdf synopsis of the medical passport.

Rule: [user] CAN [access] [data of the data subject] IF [token_data subject] [provided]

Thanks to the website address and the token provided by Stefania, DocCharly may access the predefined pdf

Scene 2:

Unfortunately, the information contained in the medical passport are insufficient to provide a correct diagnosis and DocCharly requires to see Stefania's full medical documentation.

The request is redirected to ENDORSE system who is in charge to evaluate if DocCharly is allowed to read Stefania's data.

In the PRDL repository the following rules is stored:

rule [user] MAY [access] [sensitive data _data subject] IF [user] [is a doctor under contract with EurA]

The system checks with the Docticare backend if DocCharly is under contract with EurA. The result is "false", hence DocCharly will be denied access to Stefania's medical files, but the system also launches scene 3 of the scenario described below.

Scene 3:

Endorse will now try to get user consent on the requested access.

IF [false] [Endorse] [send predefine sms to data subject]

Stefania receives a SMS with the requested data access. She confirms that DocCharly is allowed to read her data for one hour (3).

IF [data subject_sms_answer]=YES THEN [User] MAY [access] [data subject's data]

Now DocCharly gets access to Stefania's medical data.

2.3 Data Life Cycle Scenarios

2.3.1 EURA_03_01 - Storage and maintenance of personal not sensitive data

Background

David, surfing the Internet, has found the Docticare portal and wants to register himself on the portal to use the services dedicated to the registered users, even if not a EurA customer (see Figure 8).

Scene 1:

David fills in the registration form in which he has to provide some non sensitive personal data such as:

name, surname, gender, birthday, nationality, address, e-mail and phone number.

He provides all the mandatory data and some data like birthday and address which are not mandatory.

Figure 8: Docticare Registration page

Scene 2:

All the data that had been provided by David are stored in a CRM area, which also stores the privacy consents David has provided.

Scene 3:

In presence of consent or dissent for the processing of personal data for marketing purposes, the personal data David has provided will be retained until he will ask for their deletion. The following

rule details this behaviour by the system.

Rule: IF ([marketing_purposes_consent] = YES OR

IF [marketing_purposes_consent] = NO) AND

([deletion_request_exist]=FALSE) THEN

[data subject's data_retention] [allowed]

In absence of consent or dissent for the processing of personal data for marketing purposes, the personal data David has provided will be retained until he will ask for the deletion of the Docticare account. The following rule again details this behaviour by the system.

Rule: IF [marketing_purposes_consent_exist] = FALSE AND

[account_deletion_request_exist]=FALSE THEN

[data subject's data_retention] [allowed]

EurA's ENDORSE repository contains the rules stated above and the ENDORSE system may check if the box consent or dissent in CRM had been marked by David during the registration process.

If one of the two boxes has not been marked and David has asked for the deletion of his Docticare account, the system sends to the CRM manager a message requesting the deletion of David's Data.

The following rule details this behaviour by the system.

IF [marketing_purposes_consent_exist] = FALSE AND

[account_deletion_request_exist]=TRUE THEN

[CRM] MUST [delete] [data subject's data]

2.3.2 EURA_03_02 -Storage and maintenance of medical data

Background

Max has entered into a Docticare contract with EurA, he has registered himself on the portal and now he wants to add his medical data to his account allowing him to consult his health data at any time and from anywhere, update or modify them, print, and authorize the doctor to view them if necessary

Scene 1:

After going through the authentication process, Max accesses his account in Docticare: he wants to fill his medical data in the Docticare 'My health book' area (see Figure 9)

He creates his personal health profile online, filling in sections with basic information on his medical history, indicating the references of his physician and of persons to be activated in emergency.

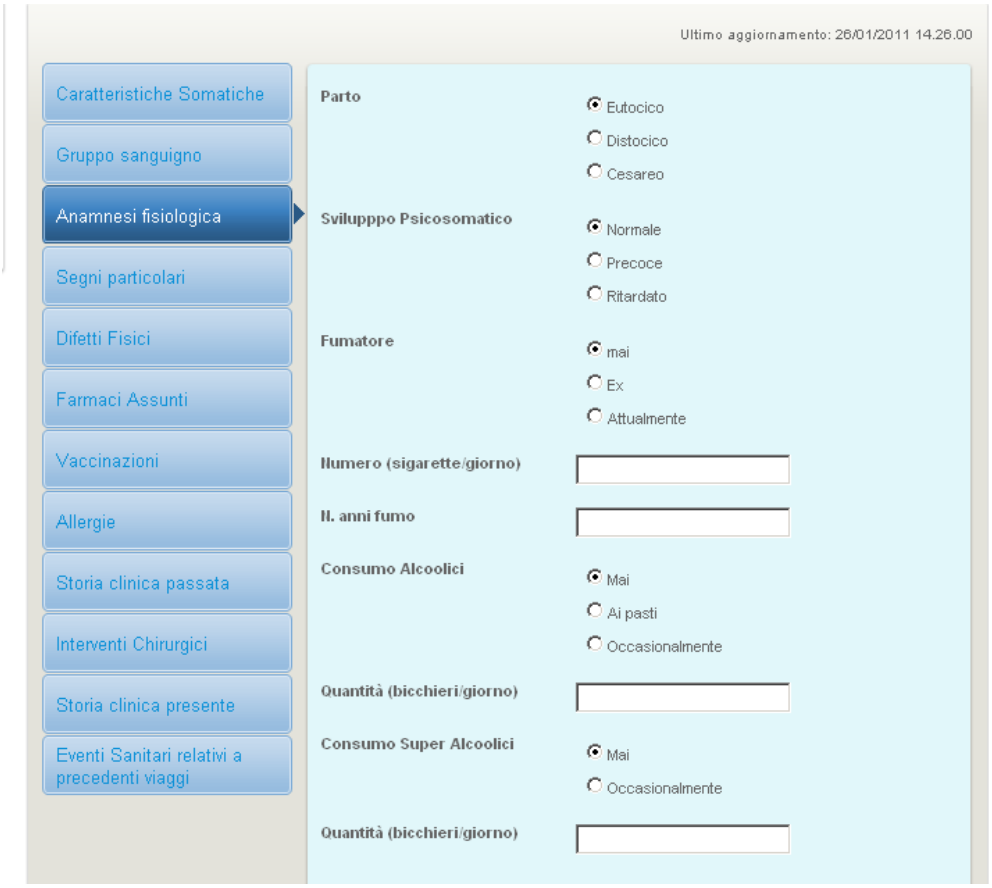

Figure 9: Medical Data Input Screen

Scene 2:

The data that are charged in 'My health book' area are marked as sensitive data and are stored on a dedicated server separated from the data subject's non sensitive personal data.

Max's health book file is associated to Max's other data in the CRM system through an ID number.

Max's health book file will be retained in the dedicated server for a period of 10 years from the contract's expiration. The following rule expresses this behaviour.

Rule: [Data Controller] MUST [retain][data subject's_data] FOR [t=contract_expiration_data+10 years]

Max's health book file may be accessed by Max through the portal for the contractual period. At the expiration date, Max will be informed that he may download his health book file within 60 days. Below the rule used in ENDORSE for this process:

Rule = [Data Controller] MUST [inform] [data subject] [about_contract_expiration_data_and_information_upload_data]

[data subject] MAY [access] [data] FOR [contractual_period+60days]

After that period Max can't access his medical data on Docticare. Obviously, if Max enters into another Docticare contract within the period of 60 day after the expiration of the previous contract, he will have available on Docticare portal the last version of his health book, since Max will continue to be EurA customer without time interruption and no data will be lost/cancelled.

Scene 3:

The EurA repository contains the rules outlined in scene 2.

The ENDORSE system allows Max's access to his Data (personal and sensitive ones) through the Docticare portal till the expiration date of the contract + 60 day.

The ENDORSE system informs the Docticare manager to send an e-mail to Max a month before the expiration term to remember him about the expiration date and the possibility to make use of the uploaded data in the following +60 days from the expiration date. There are two ways to do this: by a subscription of a new Docticare contract or by downloading the files in a pdf format.

The ENDORSE system informs the Docticare manager to delete Max's sensitive stored data 10 years after the last expiration of the contract subscribed by Max.

2.3.3 See_03 setting up account

Background: Mary has registered an account at the Seecomms Communicator (see D2.1 3.3.1 Registration). She now wants to configure her account.

Scene 1:

Mary enters her personal details in the Communicator's extensive user profile. She enters her name, address, contact details, affiliation, gender, date of birth, etc. Obviously, she does not want this information to be available to all Seecomms' users, hence she has to set up some access control policies.

Scene 2:

Mary decides to use the 'group contacts' facility in Communicator to control access to her data. She has decided to group her contacts into four distinct groups for now: family, close friends, acquaintances, colleagues. She creates the four groups in the system (see Figure 10).

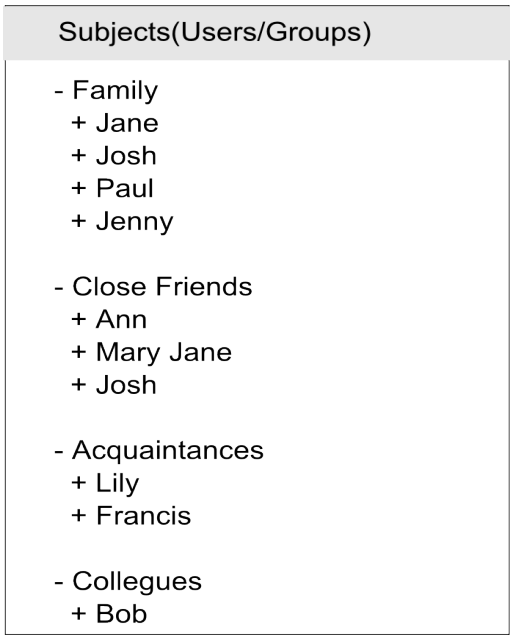

Figure 10: Users groups inside Communicator

Scene 3:

Mary goes through her address book in Communicator and assigns each of her contacts to one or more groups. Her Mom, Jane is placed in the Family category.

Scene 4:

Her brother Josh, whom she considers one of her closest friends is added to both 'family' and 'close friends'.

Scene 5:

Mary can now assign access rights to her profile data on the basis of the groups created. She decides that her family members have access to most of her data. Her colleagues, in contrast, don't get access to her home address and private preferences. To implement her policy preferences, she selects a field in her profile and drags the groups that get access to this data to the 'access granted' box. This means that users assigned to this group by Mary will be able to see the data and also to search for Mary in the system on the basis of the information in this field.

Scene 6:

Mary also wants to grant individual access to her home address to her close colleague Bob. Her colleagues can not see or search for her home address. By dragging Bob to the 'access granted' box associated to the 'home address' field, Bob is handled as an exception.

Scene 7:

Mary has a row with her aunt Jenny. Mary recently moved and she decides that Jenny does not need to know where she lives. Because Jenny is in Mary's family group of contacts, she would reason of the policy set in SEE_01_05 by default have access to Mary's address. By dragging Jenny to the 'access denied' box associated to the 'home address' field, she creates an exception for aunt Jenny.

Scene 8:

Mary is always interested in talking to people about new job opportunities, hence she decides to make the field "job qualifications" accessible by all Seecomms' users.

2.3.4 See_04 Adding contacts

Background: Mary is new to the Seecomms system, so she only has a few contacts of whom she knows that they are also Seecomms users (such as Jane, Jenny, and Josh). She decides to find out who else on the system she might know.

Scene 1:

First she decides to probe for colleagues. She pulls up the search screen and enters her company name in the search field. The query returns 4 results. She inspects the names and adds the familiar ones to her address book and marks them as colleagues.

Scene 2:

One of the newly added colleagues, Richard, has to be denied access to her "date of birth" field, she does not want him to know her age. Hence, she brings up her profile and adds Richard to the 'denied access' box of the "date of birth" field.

2.3.5 See_05 School use cases

Background: Anna wants to communicate with her class members and share her information with all except the bully Raimund. She grants access for her classmates by creating a group and define the group policy. Although Raimund is in the group classmates she explicitly drag him into a box that assures that no data is shown to him.

Scene 1:

To keep in touch with other classes, Anna wants to communicate with students from other classes but the information she shares is limited to Name, class and year. She creates a group for other

classes that handles that only the limited data is shown to group members.

Scene 2:

In addition, Anna wants to communicate with a friend in another school. The school has been defined as partner school. The students are allowed to communicate so Anna can add her friend and define what information to share with him. If the school would not be defined as partner school, Anna would not be able to add her friend.

Scene 3:

Anna has been ill and wants to ask her teacher what she has teached the class during the last week. The teacher is related to Anna's class and therefore she is allowed to add her to her contacts. She can only see what the teacher his explicitly granted what she wants the students to see.

Scene 4:

A teacher wants to communicate with a class she is responsible for and where she teaches. She creates a group for the class and adds all class members. In addition, she explicitly allows her students to see her date of birth and address.

Scene 5:

The teacher also uses SeeComms to communicate with her teacher colleagues. She also creates a group for her fellow colleagues and grants access to her telephone number as well as email and address. She excludes a colleague she doesn't like from the group.

Scene 6:

A teacher has to substitute a lesson for another student and therefore ask the headmaster for permission to add the students to her SeeComms. The headmaster grants the access and she creates a new group and adds alle the students of the class. After one week her access expires and the group will be deleted.

2.3.6 See_06 military use cases

Background: Regiment member David wants to communicate and share information with other members of his regiment. He creates a folder and adds his collegues. To limit the data share he only shares his name and email address.

Scene 1:

A fellow regiment member who is David's best friend is granted full access to all the data that David has within the system.

Scene 2:

David's family is very interested in the collegues of him. They want to contact also other members of his regiment. The regiment member can define the data that the other families are allowed to see and what explicitly is very sensitive data.

Scene 3:

David's superior wants to view some information about David and his fellow members int the regiment. The superior has access to all the data except the highly sensitive medical data. David can decide which data the superior is not allowed to see.

Scene 4:

David has a friend that is part of another regiment. To keep in touch with the friend and to share information David wants to add him to the communicator. As communication between regiments can imply information leaks David has to get this operation granted by his superior.

2.3.7 See_07 medical use cases

Background: John Doo has an accident and is transported to the local hospital. The hospital has the SeeComms system and check that John is also a user. The doctors can retrieve important information from the system, such as blood group and allergies to treat John the right way.

Scene 1:

John has defined a group of doctors in his SeeComms profile that he regularly visit as a patient. He has granted these doctors access to his medical data. A doctor which is part of that group can now access the data.

Scene 2:

John wants to get a vaccination at a hospital. The nurse would need the information when John's last vaccination had been in order to give the right dose. John grants her access to the medical data that is stored within the SeeComms system. The nurse also checks if John has any allergies against the ingredient of the vaccination.

Scene 3:

John has some friends which he trusts and therefore wants to give them access to his medical data. The friends are already in the group friends but John gives explicit access to every one. These friends are now marked as further authorized.

2.3.8 See_08 Law enforcement

Background: One of the Seecomms users is suspected to be involved in a brutal robbery of a petrol station along the M1 (how do we know?). Video footage of the petrol station's CCTV shows this person to make a call on his mobile. The police wants to know whether a call was made using Seecomms' system. DI Jones is on the case.

Scene 1:

DI Jones approaches Seecomms operator Anton with a warrant asking for the traffic data of WilliamTQ, one of Seecomms' users. Anton inspects the warrant and as it seems real informs Seecomms legal staff. Senior Legal staffer Knick decides the request is acceptable and process the request by entering his key into the traffic data system search screen, enters his own name and key as responsible officer, the requested username, and checks the 'warrant approved' field. The query is executed and produces information about WilliamTQ's calls.

Scene 2:

On the basis of this information, Di Jones requests information about all calls made at the petrol station around the time frame of the robbery.

2.4 Reporting on data usage scenarios

2.4.1 EURA_04_01 Response to a Data Subject's exercise of rights

Background:

Mark, a data subject, has received a promotional offer from EurA. He wants to know which Personal Data are stored in EurA servers.

He writes an e-mail to the EurA's Data Protection Office.

Scene 1:

Giulia, EurA's Data Protection Officer, receives Mark's request sent by e-mail: Mark wants to know what data EurA has about him. Mark provides his name and surname.

Giulia has to check if there are in EurA servers some personal data of Mark.

Scene 2:

Giulia fills in an ENDORSE form (Figure 11) with the data provided by Mark.

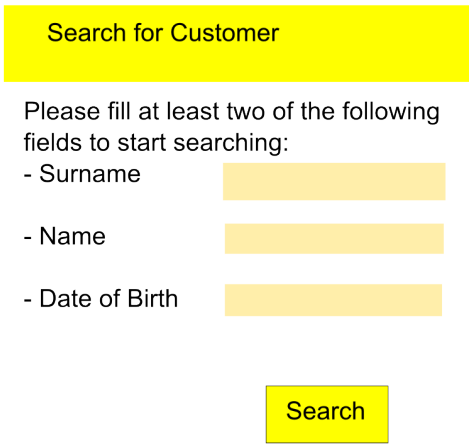

Figure 11: Search for personal data window in Endorse

Scene 3:

ENDORSE, starting with Mark's data inserted by Giulia, checks where and which are Mark's data processed by EurA.

Scene 4:

The system can't find an univocal match between the data provided by e-mail by Mark and entered in Endorse by Giulia.

Giulia writes an e-mail to Mark asking him to send a copy of his Identity Card and to specify – if known – when and in which way he has entered in a contact with EurA (through a subscription of an insurance policy, or a contract, or at a tourism fair..)

When Mark's answers, Giulia inserts in Endorse all the known data of Mark.

Scene 5:

Endorse finds an univocal match between the data inserted by Giulia and the ones stored in EurA servers.

Endorse gives to Giulia a list of the Data and of the contracts Mark has subscribed with EurA:

Mark White

via Rossi 34 – Milano

mark.white.1@yahoo.it

contracts: none date of subscription:--/--/----

claims: none date: --/--/----

Endorse gives also Mark's privacy position:

source of data: competition “Click-on Docticare”

Privacy consent:

contractual YES

commercial for EA Italia YES

commercial for EA Service YES

customer satisfaction NO

The system provides also a scan of the document in which privacy consents have been provided.

Scene 6:

With the information provided by the system, Mark receives by e-mail a pdf subscribed by the Data Protection Processor with the necessary informations.

2.5 Endorse and back-end systems interactions Scenarios

2.5.1 EURA_05_01 Data deletion when the obligation to maintain acts expires

Background: Civil law requires to maintain data for a certain periods, privacy law to maintain data for no longer than is necessary for the purposes for which the data were collected or subsequently processed.

Scene 1: John has subscribed a Docticare contract with EurA on 15/05/2001. The contract had expired on 14/05/2002 and has not been renewed.

During the contract period John has provided the Docticare portal with his medical data that had been stored in the dedicated area of EurA server.

At the subscription John has given his consent to EurA for commercial purposes.

Scene 2:

After the contract expiration date:

John's medical data has to be maintained in EurA dedicated server for 10 years till to 14/05/2012

John's non sensitive data, in presence of his consent for marketing purposes, has to be maintained in EurA CRM.

Scene 3: Every day at 00:01 the ENDORSE system evaluates the expiration of the rights to keep personal data

The following rules, stored in the rule repository, are automatically evaluated:

[DC] MUST [check] IF [claim_opening_exist]= TRUE THEN

[DC] MUST [delete] [data] [at_claim _closure_date+10 years].

[DC] MUST [check] IF [claim_opening_exist]= FALSE THEN

[DC] MUST [delete] [data] [at_contract _expiration_date+10 years].

Scene 4: Based on the evaluation of the rules , the system provides the database management system a list of EurA personal data to be deleted. The list is taken in charge by the DBMS which provides the desired data deletion.

2.5.2 EURA_05_02 Endorse integration with other Back-end systems.

Background: EurA uses an internal document management platform for different purposes. In this case we describe a possible integration among the Claim system, the document management system and a third party company engaged by EurA for storing paper documentation. Opening a claim implies that the customer can send different documentation on different media (e.g. fax, @, upload of scanned docs, etc.). These media are integrated with the document management system which stores these data under the claim identification number. Paper docs can either be sent to EurA by the customers. In these case the paper docs are stored in a third party warehouse and can be required by the company offices on demand.

Scene 1: EurA is requested to open a claim on contract XX. The claim system creates the claim identification number (dossier) which is immediately notified to the ENDORSE component.

Scene 2: EurA receives a fax containing medical invoice regarding contract XX. This document is stored into the document management system under the dossier number. The document management system immediately notifies the ENDORSE component that it has got a document regarding the claim.

Scene 3: EurA receives a paper document regarding contract XX by the customer. This document is stored into a paper dossier which is then sent to the third party warehouse. The ENDORSE component is notified of this operation.

Scene 4: Once the claim has been closed, the Claim management system notifies ENDORSE of the claim closing date. Note that the claim may be reopened; in this case the Claim management system notifies Endorse of the claim reopening and that the previous closing date is not longer valid. Endorse calculates and stores the date when all the claim data can be deleted (10 years after the claim closing).

Scene 5: At the deletion day ENDORSE notifies all the systems involved in the claim management that the related data must be cancelled. Each system involved in this task has to provide feedback to Endorse that the task has been completed. ENDORSE will continue, on a periodical basis, to send an alarm to the systems which have not provided feedback on the deletion task.

3 Conclusion

In this deliverable we have presented a set of scenarios useful to describe how ENDORSE will change the way data privacy is managed by European Companies.

There are 5 sets of scenarios divided on the basis of the main topic they cover. Another important division is due to the Company which is the environment of the scenario itself.

Scenarios were based on two Company situations: one, Europ Assistance, is an insurance company with one product, Docticare, devoted to medical assistance, the other one, Seecomms, is a communication company whose main product is a kind of social network with many different situations in which personal data are gathered, stored or, in case, transmitted to third people.

Unfortunately Seecomms, due to internal reasons, decided to leave the Endorse project at the end of may. This deliverable treasured the experience gained during the months of work with Seecomms but was edited and completed by Europ Assistance and Soluta.Net who helped the task 2.4 leader to finalise this effort.

The scenarios provided in this deliverable and the output of the legal requirements task and the social requirements task in work-package 2 provides the final input for the developers of the PRDL (Privacy Rules Definition Language) and the (software) developers of the policy system. This document provides a example-based idea of what the language should be capable of expressing and where and how the policy system can fit into existing and future systems.

